智能仿真与攻击诱捕工具

DecoyMini

用户手册

目 录

1 背景

随着以数字化、网络化和智能化为特征的信息化浪潮的蓬勃兴起，信息已经成为重要的战略资源与重要生产要素，在国家的发展和人们的生产生活中起到至关重要的作用。信息化在给人们带来便利的同时，网络信息安全问题也日益凸显。经过多年的网络安全基础设施的建设，安全防护系统经历了从无到有、从有到全的发展过程，防火墙、IDS、漏扫、杀毒软件、流量监测等安全产品应运而生，构成了庞大而复杂的安全防御体系，但是尽管如此，针对网络的风险事件却依然频发，APT 攻击、蠕虫木马、勒索、挖矿、敏感数据泄露等安全事故更是层出不穷。网络攻击由传统的盲目、直接、粗暴的方式转变为目前的精确化、持久化、隐匿式的恶意攻击，攻击者通过有组织、有策略的步骤和方法达到攻击目的。攻击过程中只需发现并利用一个未被修复的漏洞或不安全配置即可击破边界防御，试图将攻击者拒之门外的被动安全防护方案在面对攻击手段的多样化、复杂化时已经力不从心。

被动防御技术已无法满足当前最新的网络安全对抗态势。一些新的安全技术不断涌现，欺骗防御就是其中主要技术之一，欺骗防御大家俗称蜜罐，它是主动防御的主要方法，是实战由被动向主动转变的最有效手段， Gartner 评价欺骗防御是对现有安全防护体系产生深远影响的安全技术，在近几年的攻防演习中被大家称为 HW 神器。欺骗防御的原理是通过构造大量虚假的网络环境、主机、服务和诱饵，引诱攻击者去访问虚假环境来及时发现攻击并对攻击者进行溯源反制，以保护客户真实资产。

2 介绍

智能仿真与诱捕防御工具——DecoyMini 是由北京吉沃科技有限公司推出的免费蜜罐软件，工具采用轻量化威胁诱捕技术，具备丰富的攻击诱捕和溯源分析能力；支持插件化的仿真模板，从论坛一键下载模板就可以快速在本地部署新的蜜罐；提供灵活的蜜罐自定义能力，通过界面可视化编排即可部署专属的蜜罐；支持本地高质量内生情报输出，可以无缝应用到网关设备对攻击进行及时封堵。DecoyMini 是企业零成本构建主动感知网络攻击的得力工具，可以协助企业有效

提升网络安全监测、响应及防御能力。

DecoyMini 具有如下特点：

- **智能仿真：**插件化的仿真模板，一键导入云端仿真模板库就可以在本地网络快速部署多样化的安全可控的仿真服务和应用，支持对 WEB 站点进行自动学习和仿真
- **高效诱捕：**支持快速部署蜜罐群，使用虚拟 IP，将网络内空闲的 IP 资源绑定到一到多个仿真环境上，支持动态绑定端口来增加蜜罐诱惑性，大大提高攻击诱捕的能力
- **灵活扩展：**采用可视化仿真编排引擎，用户通过界面配置即可实现对自定义的网络协议、服务或应用的仿真，模板支持系统间快速迁移和通过 DecoyMini 论坛进行分享
- **部署简便：**支持主流操作系统（Windows 32/64 位，CentOS/Ubuntu/Debian/Kali 32/64 位，树莓派等）,支持 Docker 运行，支持单节点、多节点集中管理，部署灵活、一键安装、使用简单
- **安全有效：**基于商业化蜜罐产品（DecoyPro）能力积累，采用轻量化威胁诱捕技术做免费蜜罐工具（DecoyMini），安全性好，成熟度高、稳定性有保障。

3 应用场景

DecoyMini 可以部署到不同的网络环境里，提供多样化的攻击诱捕能力。典型的应用场景介绍如下：

3.1 互联网攻击诱捕分析

面对互联网攻击频繁，各种高级、隐蔽的攻击层出不穷；而用传统安全设备很难有效防御，安全运维人员应付起来也是疲于奔命。

通过部署 DecoyMini，利用丰富多样的仿真模板，部署典型的蜜罐映射到外网，提供常态化的外网攻击感知能力；也可以利用自定义蜜罐能力，将个性化的蜜罐映射到外网，对互联网上尝试攻击我方的攻击源进行诱捕和监测；支持与网

关设备联动来及时对外部攻击进行处置和阻断，提升对外部攻击的处置和响应能力。

3.2 内网横向攻击监测预警

通常内网的访问控制都不严格，攻击横向移动比较容易；而内网系统往往漏洞未能及时修补、弱口令威胁也相当严峻，极易遭受恶意的攻击。

通过部署 DecoyMini，在内网部署一些常用的应用、服务蜜罐，并开启网络扫描、连接监听等功能，就可以提供常态化的内网横向攻击监测感知能力，可以及时发现感染勒索、挖矿、蠕虫等病毒木马的失陷主机，潜伏到内网的攻击者，以及内部人员发起的各种攻击行为。

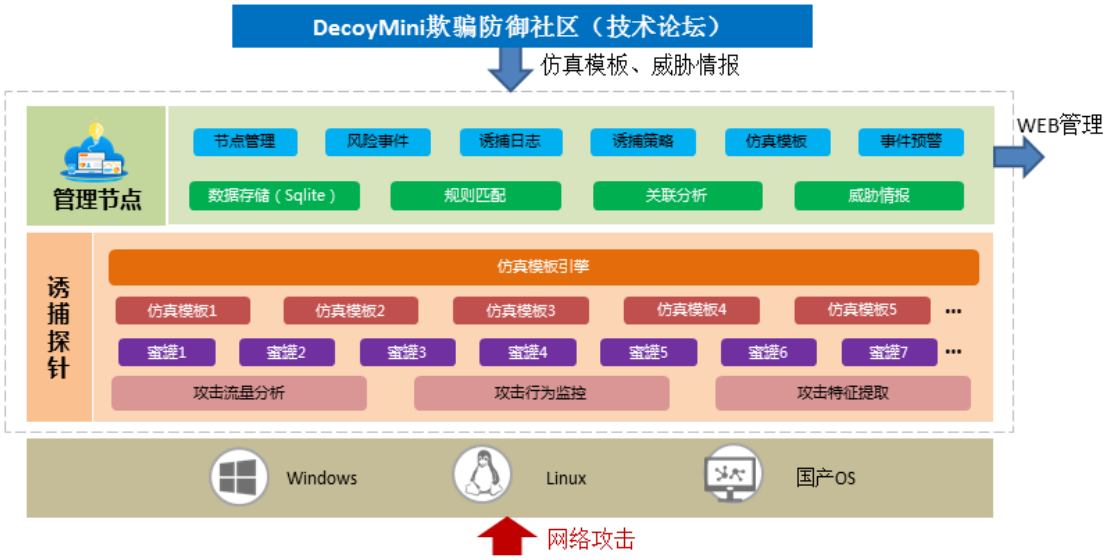
3.3 网络攻防对抗演习监测

近几年来攻防演习常态化进行，在攻防演习中需要有手段能够对红队的攻击进行监测、对攻击的进展进行跟踪，同时对攻击行为进行溯源反制。

通过部署 DecoyMini，可以对红队的攻击行为进行监测，支撑对攻击套路进行分析，用以指导蓝队制定更为有效的防御措施；同时，用蜜罐为载体构造场景可以来投递溯源、反制工具，实现对红队的溯源。结合攻击的完整日志和攻击者画像，协助完整溯源攻击链，获得溯源得分。

4 系统架构

DecoyMini 包括诱捕探针和管理节点两大组件，架构图如下所示：



诱捕探针内部包含了一个基于软件仿真技术的仿真模板引擎，它接收管理节点的诱捕策略，调度对应的仿真模板来部署蜜罐，对各种针对蜜罐的攻击行为和攻击流量进行监测和记录，对攻击者的特征信息进行提取，将采集到的这些数据统一上报到管理节点进行集中分析。

管理节点提供 WEB 方式的管理入口，提供仿真模板配置、诱捕策略下发、诱捕日志查询、风险事件管理等管理功能；负责下发诱捕策略，同时接收诱捕探针上报的各类数据，存储到本地 Sqlite 数据库，并通过规则匹配、威胁情报、关联分析等分析手段识别关键攻击行为，生成风险事件；通过从云端自动下载仿真模板和威胁情报库来持续更新本地的攻击诱捕能力。

5 部署

5.1 部署模式

产品支持如下两种部署模式：

- 单节点模式：管理节点与诱捕探针一体化运行在一台主机上，为 DecoyMini 默认模式。
- 集中管理模式：在网络中选择一台主机部署 DecoyMini 软件作为管理节点，在多个主机上以诱捕探针模式部署诱捕节点，将诱捕节点集中到此管理节点统一管理。

5.2 环境需求

5.2.1 硬件配置

配置/类别	单节点	管理节点	诱捕探针
最低配置	CPU ≥ 2 核; 内存 ≥ 1G; 硬盘 ≥ 20G	CPU ≥ 2 核; 内存 ≥ 2G; 硬盘 ≥ 100G	CPU ≥ 1 核; 内存 ≥ 1G; 硬盘 ≥ 10G
推荐配置	CPU 4 核; 内存 2G; 硬盘≥ 50G	CPU 4 核; 内存 4G; 硬盘≥ 200G	CPU 2 核; 内存 2G; 硬盘≥ 20G

5.2.2 网络端口

序号	类别	端口	协议	描述
1	管理端口	安装时自定义	TCP	用于 DecoyMini 系统管理 DecoyMini 部署为单节点/管理节点模式时使用
2	业务端口	1226	TCP	用于诱捕探针状态管理、策略下发、数据采集
3	蜜罐端口	诱捕策略定义	TCP/UDP	用于部署蜜罐

5.3 软件下载

前往以下地址下载最新版本的 DecoyMini 安装包：

- https://github.com/decoymini/DecoyMini/releases
- http://decoymini.decoyit.com

DecoyMini 支持主流操作系统部署（包括：Windows 32/64 位,CentOS/Ubuntu/Debian/Kali 32/64 位,树莓派等），支持 Docker 运行。

5.4 单节点/管理节点安装

5.4.1 Windows 下安装

Windows 下，以管理员身份运行 cmd，输入如下命令开始安装：

```
DecoyMini_Windows_v1.0.xxxx.exe -install
```

按需选择 DecoyMini 管理端监听的地址和端口后，完成 DecoyMini 的安装。

5.4.2 Linux 下安装

Linux 下安装，以 CentOS 64 位为例，对安装文件赋予可执行权限，用管理员权限执行如下安装命令：

```
./DecoyMini_Linux_x64_v1.0.xxxx.pkg -install
```

按需选择 DecoyMini 管理端监听的地址和端口后，完成 DecoyMini 的安装。

5.4.3 Docker 下安装

在已安装 Docker 的环境下，运行如下命令快速安装 DecoyMini：

```
docker run -itd --name decoymini \
 --network host \
 --restart=always \
 --privileged=true \
 decoyit/decoymini:latest
```

使用 Docker 镜像安装 DecoyMini，默认管理端口为 88，可以通过设置环境变量 LISTENING_ADDR 来更改监听端口；可以将 DecoyMini 的 /usr/decoymini 和 /usr/decoy 两个目录持久化，实现 DecoyMini 系统数据持久化存储。

支持自定义监听端口和数据持久化的安装命令如下：

```
docker run -itd --name decoymini \
 -v /usr/decoymini:/usr/decoymini \
 -v /usr/decoy:/usr/decoy \
 --env LISTENING_ADDR="0.0.0.0:8090" \
```

```
--network host \
--restart=always \
--privileged=true \
decoyit/decoymini:latest
```

注意：按需将环境变量 LISTENING_ADDR 的值更改为实际需要监听的地址和端口。

5.5 诱捕探针安装

5.5.1 Windows 下安装

Windows 下，以管理员身份运行 cmd，输入如下命令完成安装：

DecoyMini_Windows_v1.0.xxxx.exe -install -addr 管理节点地址

示例：

DecoyMini_Windows_*.exe -install -addr http://192.168.8.100:8080

5.5.2 Linux 下安装

Linux 下安装，以 CentOS 64 位为例，对安装文件赋予可执行权限，用管理员权限执行如下安装命令：

./DecoyMini_Linux_x64_xxx.pkg -install -addr 管理节点地址

示例：

./DecoyMini_Linux_ x64_*.pkg -install -addr http://192.168.8.100:8080

5.5.3 Docker 下安装

在已安装 Docker 的环境下，运行如下命令快速安装 DecoyMini 诱捕探针：

```
docker run -itd --name decoymini \
 --env MANAGER_ADDR="http://192.168.1.100:88" \
```

```
--network host \
--restart=always \
--privileged=true \
decoyit/decoymini:latest
```

注意：须将环境变量 MANAGER_ADDR 的值更改为实际管理节点部署的地址。

5.6 命令行升级

产品支持管理端升级和命令行升级两种操作模式，管理端升级配置参见“系统/自动升级，手动升级”章节，以下介绍管理节点和诱捕探针命令行升级操作方法。在已安装管理节点和诱捕探针的主机上：

Windows 下，以管理员身份运行 cmd，输入如下命令完成升级：

```
DecoyMini_Windows_v1.0.xxxx.exe -upgrade
```

Linux 下安装，以 CentOS 64 位为例，对安装文件赋予可执行权限，用管理员权限执行如下升级命令：

```
./DecoyMini_Linux_x64_xxxx.pkg -upgrade
```

5.7 软件卸载

Windows 下卸载，以管理员身份运行 cmd，输入如下命令完成卸载：

```
decoymini .exe -uninstall
```

Linux 下卸载，用管理员权限在终端下输入如下命令来完成卸载：

```
decoymini -uninstall
```

5.8 其它命令

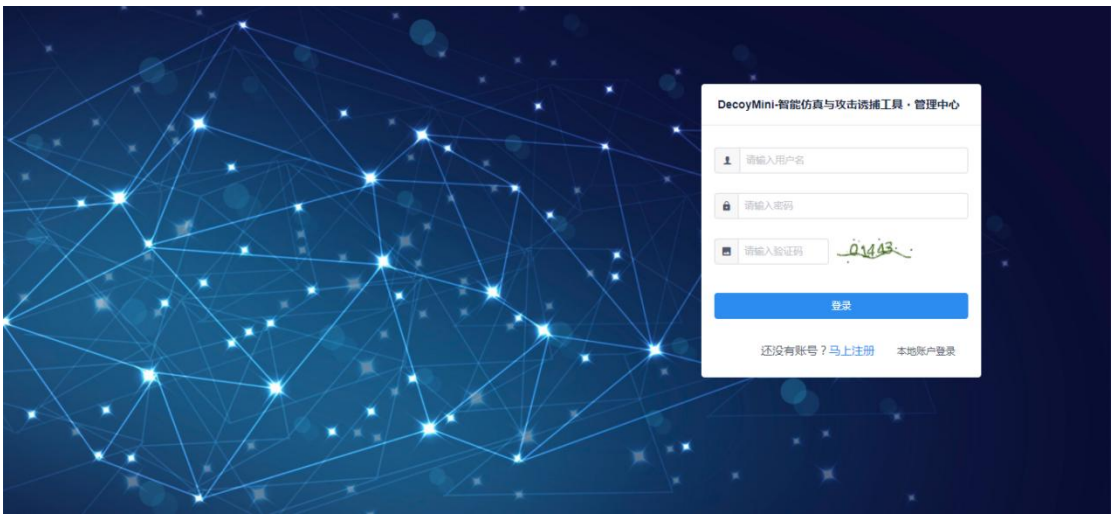
```
Usage of DecoyMini:
  -info
        Show information          //显示 DecoyMini 安装信息
  -set -addr string
        Set Manager address       //更改诱捕探针的管理节点地址
  -uninstall
        Uninstall Software
```

示例：更改诱捕探针管理节点地址为 http://192.168.8.200:8080，在命令行窗口执行如下命令：

```
decoymini -set -addr http://192.168.8.200:8080
```

5.9 系统登录

安装完成后，使用安装 DecoyMini 时配置的 IP 和端口即可访问管理端，若采用默认安装，访问 http://127.0.0.1 即可登录管理端，界面如下所示：



系统支持两种登录方式，一种是使用论坛账户直接登录（推荐使用），另一种是使用本地默认账户登录。

可访问互联网的环境，推荐注册论坛账号登录，支持一个账号管理多个 DecoyMini 系统，同时 DecoyMini 与欺骗防御技术论坛无缝衔接、支持论坛自动登录，仿真模板一键下载、一键升级等功能。

本地默认账户密码为：

账户：admin

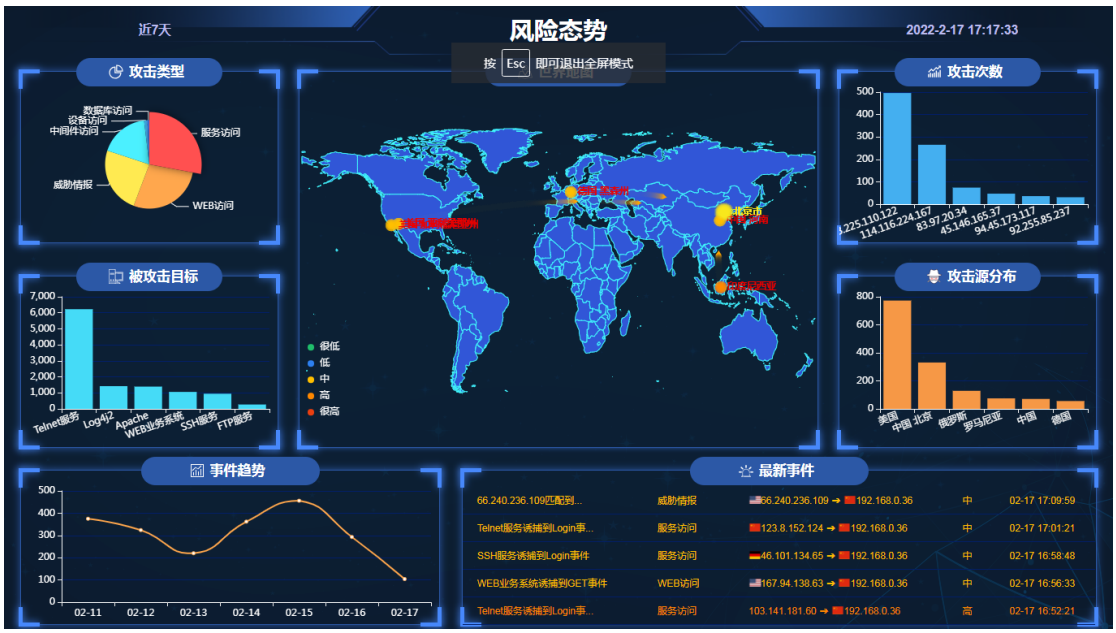
密码：Admin@123

功能介绍

1 监控

1.1 风险态势

提供系统风险态势集中监控的功能，可查看“攻击类型”、“攻击次数”、“被攻击目标”、“攻击源分布”、“事件趋势”、“最新事件”等分布图，如下图所示：



1.2 仪表盘

仪表盘主要用于展示系统的关键指标和数据，以图表等可视化的形式来进行展示。点击 "监控" --> "仪表盘"，进入仪表盘界面：

主要展示以下信息：

- 事件数量分布：统计最近一段时间内发生的风险事件的数量分布情况；
- 事件级别占比：展示的为根据风险事件的风险级别统计的结果；
- 事件类型 TOP10：展示的为根据事件类型统计的 Top10 排名；
- 日志级别占比：展示的为根据诱捕日志的各个级别统计的结果；
- 日志类型 TOP10：展示的为根据日志类型统计的 Top10 排名；
- 诱捕器日志数量 TOP10：展示各诱捕器产生的日志数量统计的 Top10 排名；
- 攻击次数 TOP10：展示的为根据 IP 攻击次数的数量统计的 Top10 排名；
- 攻击源分布 TOP10：展示的为根据攻击者来源的地域统计的 Top10 排名；
- 攻击用户 TOP10：展示的为根据攻击者使用的攻击用户名统计的 Top10 排名；
- 攻击操作 TOP10：展示的为根据攻击者的攻击动作统计的 Top10 排名；

可以点击右上角时间选择按钮，选择今天、最近 24 小时、最近 3 天、最近 7 天、最近 30 天、指定时间段，来展示对应时间范围内的统计数据。

报表导出：可导出 PDF 格式报表。

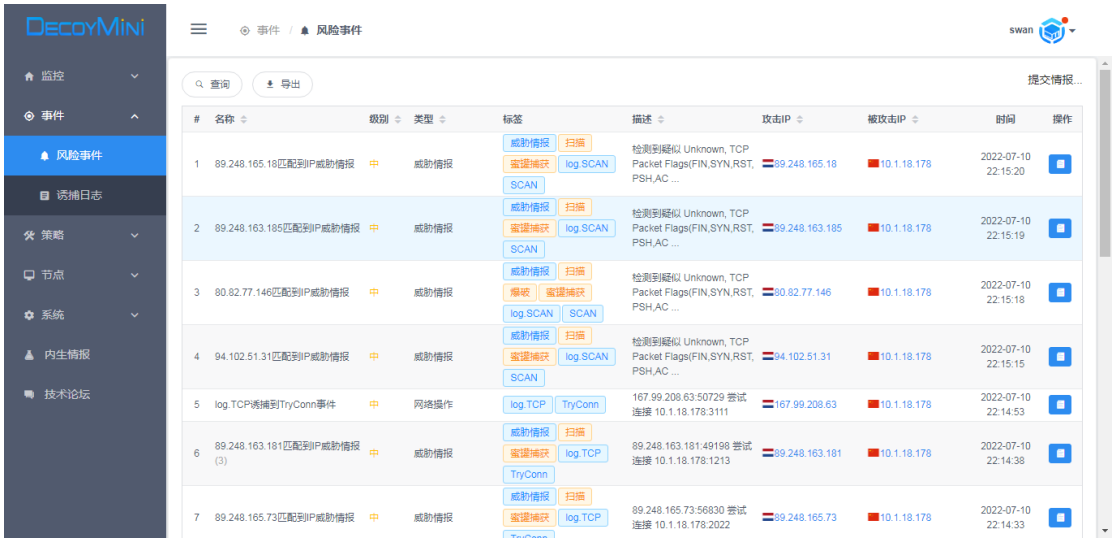
2 事件

事件主要提供对系统产生的风险事件进行查询、管理，对系统诱捕到的诱捕日志进行查询管理的功能。

2.1 风险事件

风险事件管理页面展示系统产生的所有风险事件信息，按时间由近到远进行展示，并提供对风险事件进行快速查询和分析的功能。

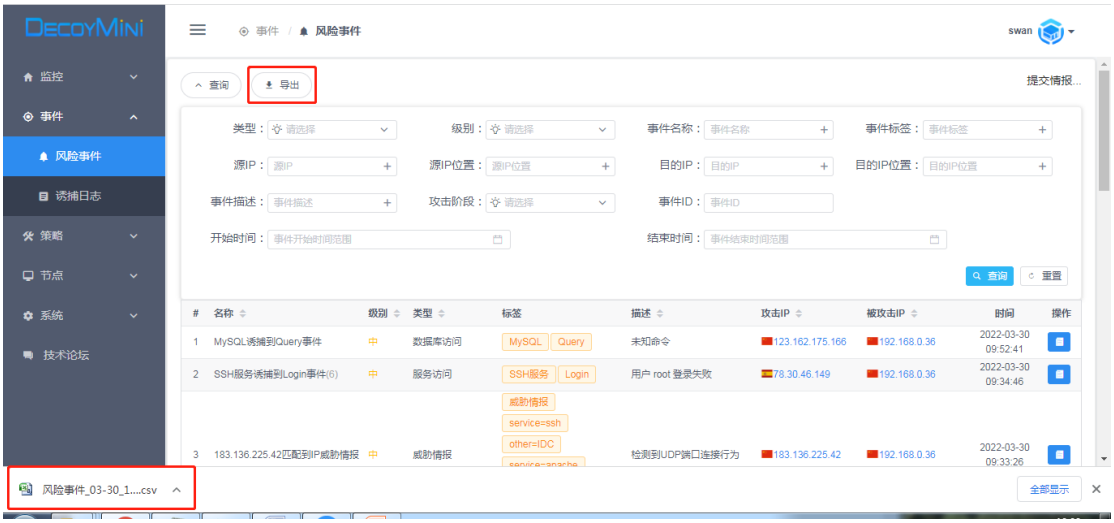
点击 "事件" --> "风险事件"，可以打开风险事件管理页面：



2.1.1 风险事件管理

点击“查询”按钮，可以根据风险事件主要属性对关注的风险事件进行查询筛选。

点击操作栏“导出”按钮，可以将当前的查询结果保存为 csv 格式下载到本地。



点击风险事件操作列 "信息" 按钮或者双击风险事件对应行，可以查看该条风险事件的详细信息，展示的信息如下图所示：

风险事件的详细信息中包含两部分内容：事件详情和关联诱捕日志。

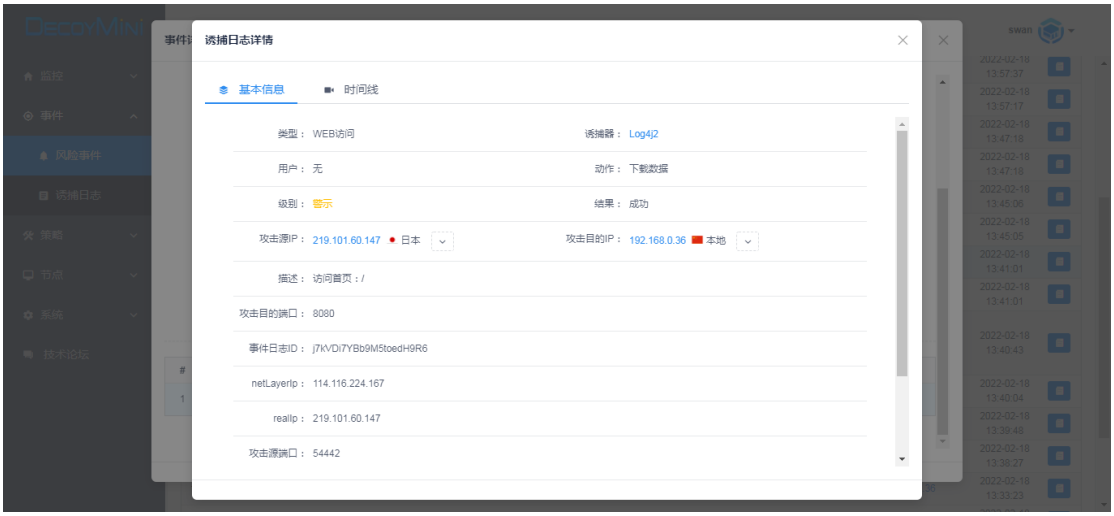
事件详情展示风险事件的名称、描述、类型、合并数量、攻击源 IP、攻击目的 IP、匹配到的关联分析规则名称、威胁影响和解决方案、风险事件合并开始时间和结束时间等属性。

点击攻击源 IP 或攻击目的 IP 后面的 按钮，将出现该 IP 的快捷操作菜单，如下图所示：

- 加全局白名单：如果该 IP 为受信任的 IP，可以将该 IP 一键加入全局白名单，所有诱捕探针节点后继将不再产生跟这个 IP 相关的事件或日志；
- 加节点白名单：如果该 IP 为受信任的 IP，可以将该 IP 一键加入节点白名单，产生此风险事件的诱捕探针节点后继将不再产生跟这个 IP 相关的事件或日志；
- 查询威胁情报平台：一键跳转到威胁情报平台查询该 IP 详细信息，系统目前预置了奇安信威胁情报中心、守望者威胁情报平台，用户可以按需在“系统”/ “参数配置”/“情报查询”里加入其他威胁情报查询平台；

关联诱捕日志展示的风险事件关联的诱捕日志列表，展示的内容如下图所示：

点击诱捕日志操作列的 "详情" 按钮，可以查看该条诱捕日志的详细信息，展示界面如下：



诱捕日志的详细信息中包含两个标签页：基本信息和时间线。基本信息是展示诱捕日志的各项基本信息，主要包括如下属性：

- 类型；
- 诱捕器名称；
- 描述；
- 日志级别；
- 攻击源 IP；
- 攻击目的 IP；
- 操作用户；
- 操作类型；

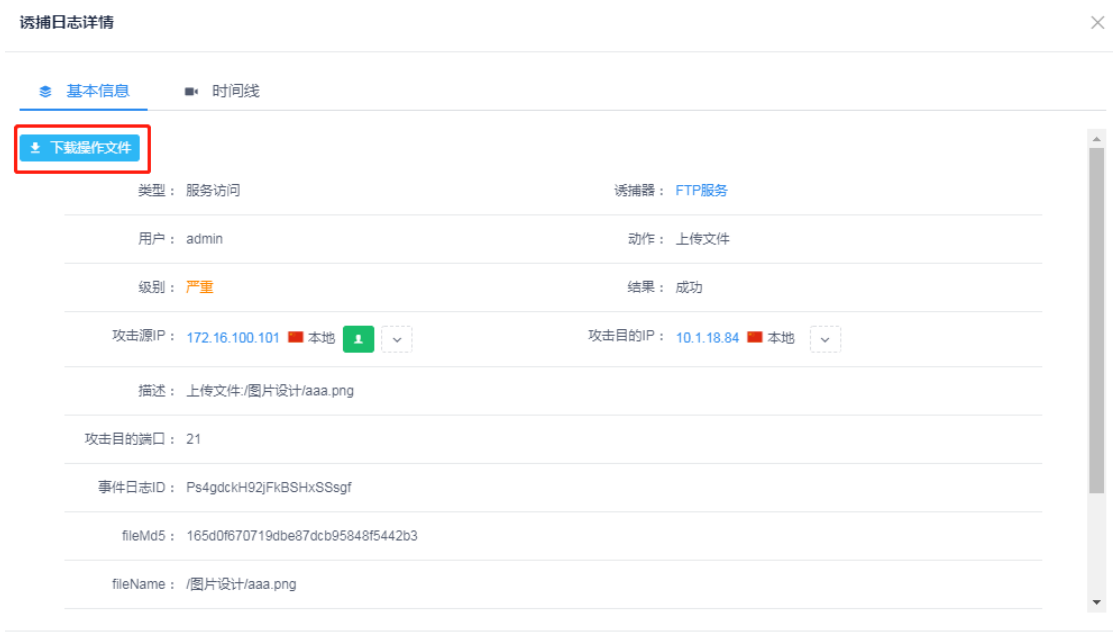
- 操作结果；
- 日志记录时间；
- 日志保存时间；

2.1.2 攻击时间线

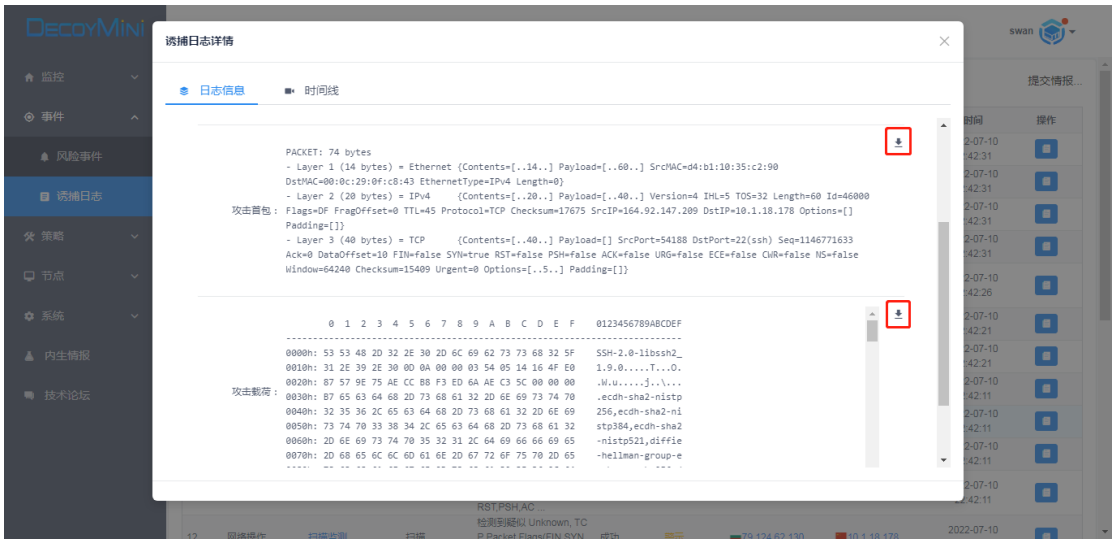
时间线是将该日志对应会话产生的所有诱捕日志以时间先后顺序来进行展示，还原攻击的完整过程。展示的界面如下图所示：

2.1.3 攻击数据下载

如果该诱捕日志为文件操作，在该日志信息操作列点击 "操作文件" 按钮可以下载对应操作的文件数据。



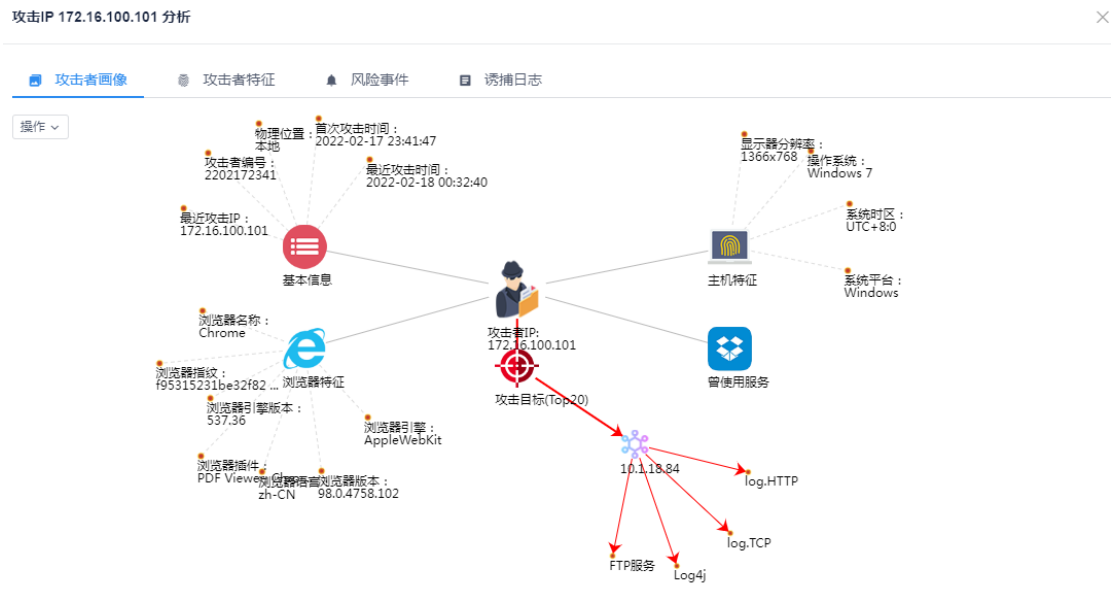
开启了 TCP 连接监测功能的，系统将记录符合条件的 TCP 攻击首包和攻击载荷数据，在诱捕日志详情里可以直接查看，也可以点击右边下载按钮来下载到本地进行进一步的分析。



2.1.4 攻击 IP 画像

点击事件列表或事件详情中的“攻击 IP”，可以展示对应攻击 IP 的画像信息。

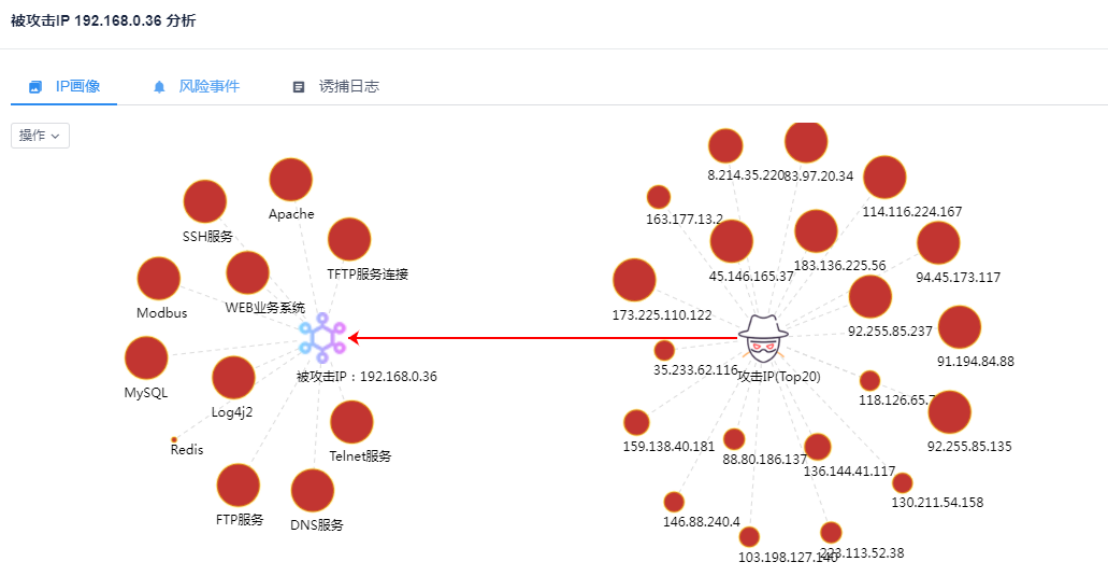
攻击源 IP 画像如下所示：



点击画像上的基本信息、主机特征、浏览器特征、曾使用服务，可以钻取到对应攻击源 IP 的攻击者特征详情；点击攻击目标的 IP 或诱捕器，可以钻取到攻击源 IP 对该攻击目标实施攻击产生的风险事件和详细诱捕日志列表。

2.1.5 被攻击 IP 画像

点击事件列表或事件详情中的“被攻击 IP”，可以展示对应被攻击 IP 的画像信息。



点击画像上的攻击源 IP 或诱捕器名称，可以钻取到对应攻击 IP 对指定诱捕器实施攻击产生的风险事件和诱捕日志列表。

2.1.6 攻击者溯源

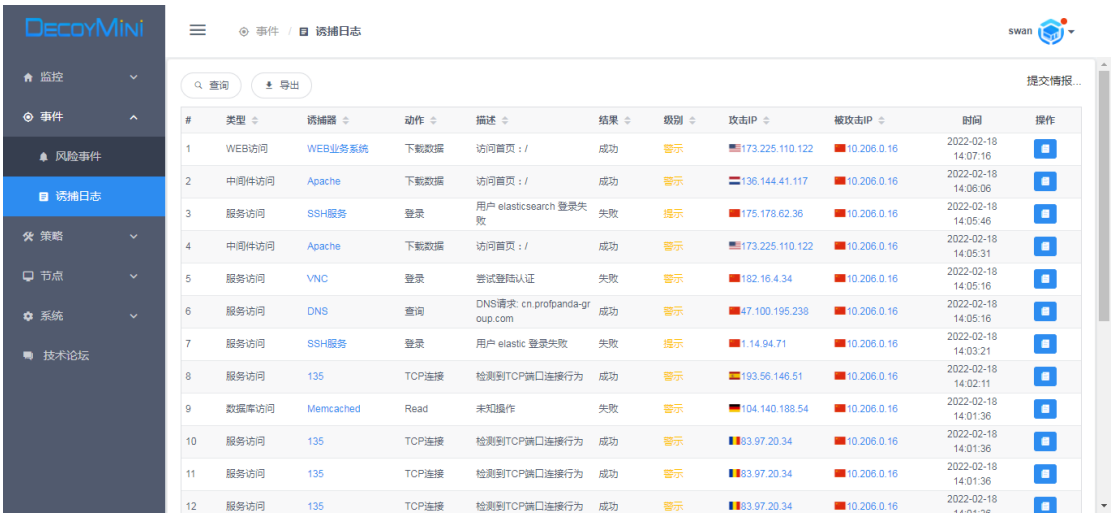
若攻击者访问诱捕器后被采集到攻击者特征信息，则攻击 IP 后会出现人像按钮，点击按钮则可以查看对应 IP 的溯源信息。

攻击者溯源信息：

2.2 诱捕日志

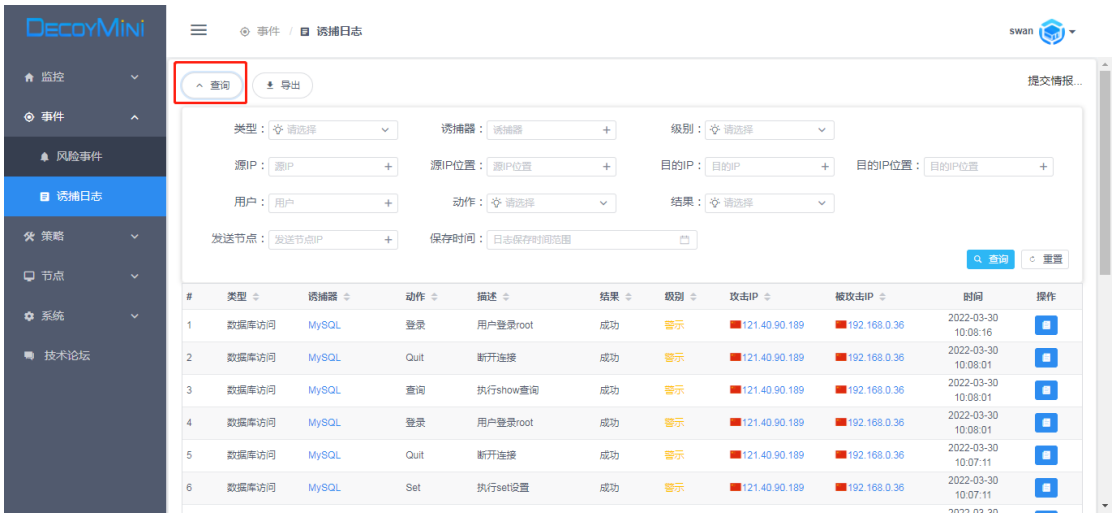
诱捕日志管理功能提供对攻击者在诱捕器中所有操作行为：包括网络操作、命令执行、文件操作以及文件等数据进行综合浏览、查询的功能。

点击 "事件" --> "诱捕日志" 打开如下页面：

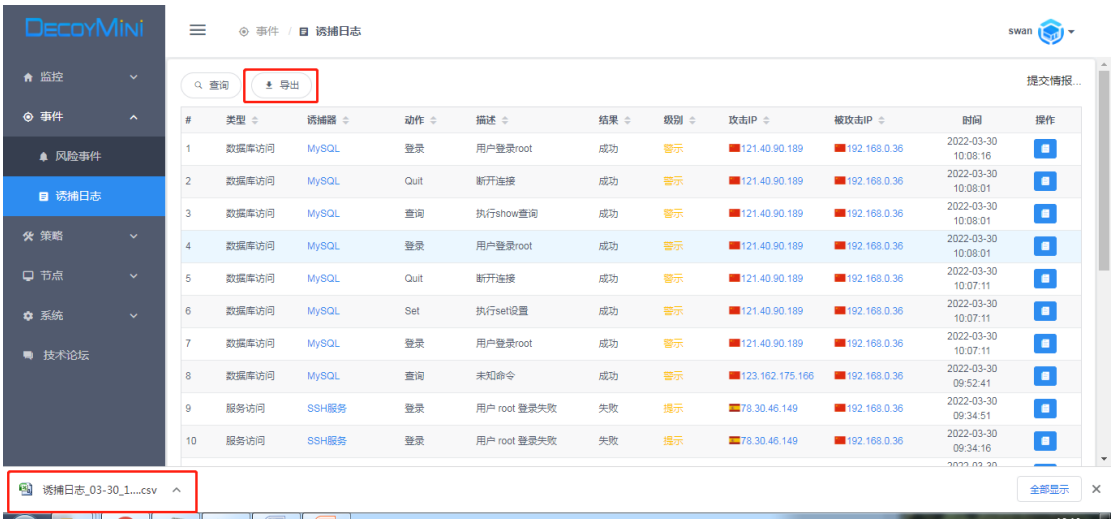


2.2.1 诱捕日志管理

点击“查询”按钮，可以根据诱捕日志主要属性对关注的诱捕日志进行查询筛选。

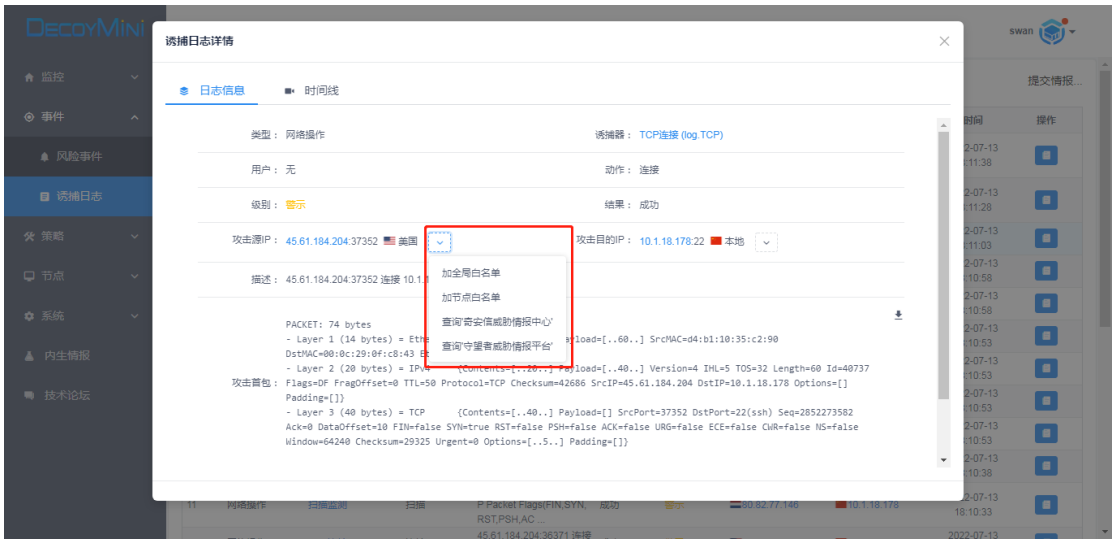


点击操作栏“导出”按钮，可以将当前的诱捕日志查询结果保存为 csv 格式下载到本地。



双击诱捕日志，可以打开诱捕日志详情。

点击攻击源 IP 或攻击目的 IP 后面的 按钮，将出现该 IP 的快捷操作菜单，如下图所示：



- 加全局白名单：如果该 IP 为受信任的 IP，可以将该 IP 一键加入全局白名单，所有诱捕探针节点后继将不再产生跟这个 IP 相关的事件或日志；
- 加节点白名单：如果该 IP 为受信任的 IP，可以将该 IP 一键加入节点白名单，产生此诱捕日志的诱捕探针节点后继将不再产生跟这个 IP 相关的事件或日志；
- 查询威胁情报平台：一键跳转到威胁情报平台查询该 IP 详细信息，系统目前预置了奇安信威胁情报中心、守望者威胁情报平台，用户可以按需在“系统”/ “参数配置”/“情报查询”里加入其他威胁情报查询平台；

2.2.2 攻击时间线

时间线是将该日志对应会话产生的所有诱捕日志以时间先后顺序来进行展示，还原攻击的完整过程，在诱捕日志详情里点击“时间线”标签，展示的攻击时间线如下图所示：

2.2.3 攻击数据下载

如果该诱捕日志为文件操作，在该日志信息操作列点击 "操作文件" 按钮可以下载对应操作的文件数据。

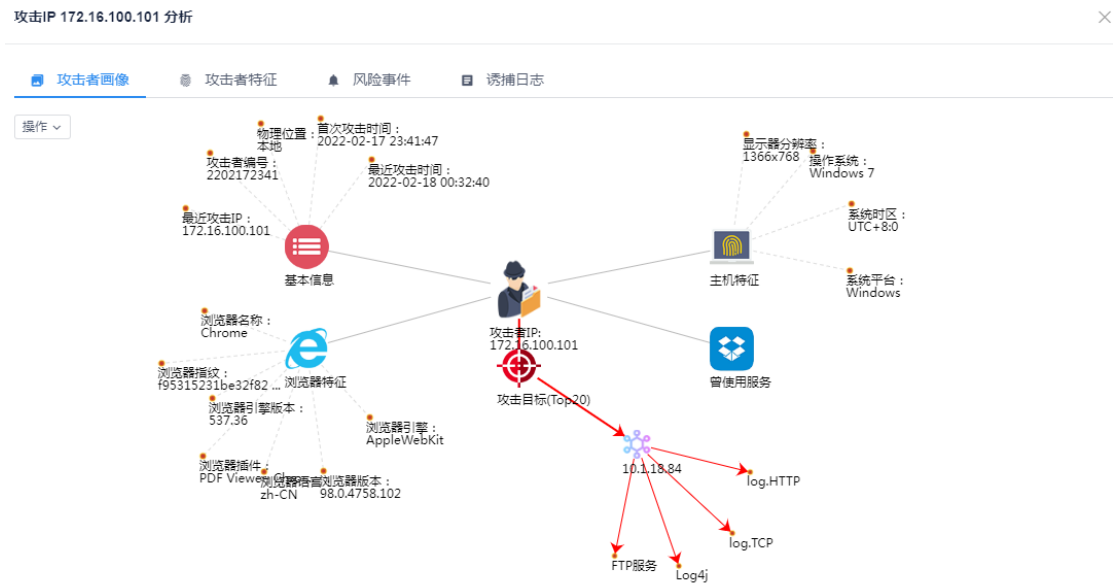
开启了 TCP 连接监测功能的，系统将记录符合条件的 TCP 攻击首包和攻击载荷数据，在诱捕日志详情里可以直接查看，也可以点击右边下载按钮来下载到

本地进行进一步的分析。

2.2.4 攻击 IP 画像

点击诱捕日志列表或诱捕日志详情中的“攻击 IP”，可以展示对应攻击 IP 的画像信息。

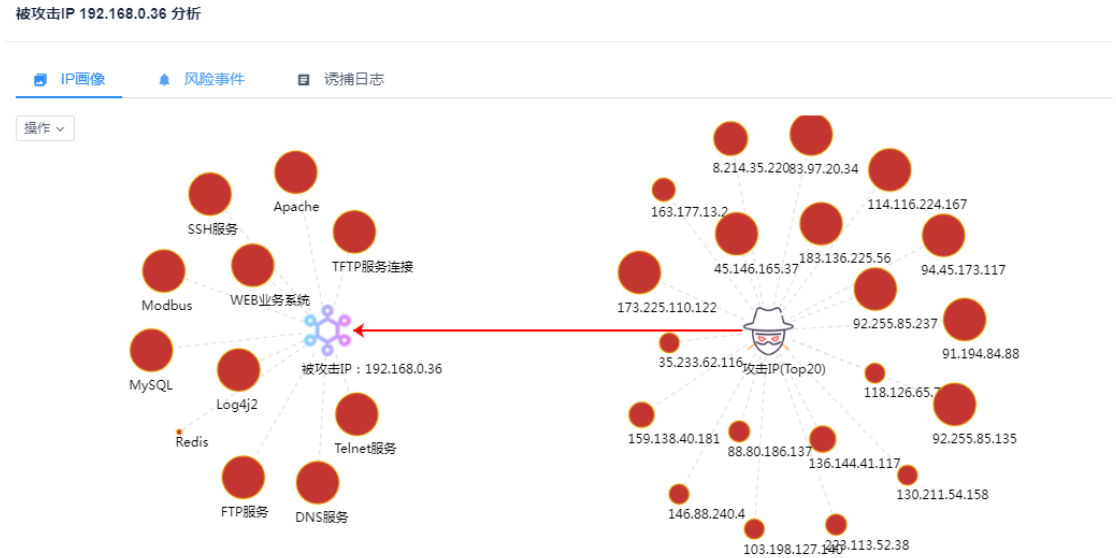
攻击 IP 画像如下所示：



点击画像上的基本信息、主机特征、浏览器特征、曾使用服务，可以钻取到对应攻击源 IP 的攻击者特征详情；点击攻击目标的 IP 或诱捕器，可以钻取到攻击源 IP 对该攻击目标实施攻击产生的风险事件和详细诱捕日志列表。

2.2.5 被攻击 IP 画像

点击诱捕日志列表或诱捕日志详情中的“被攻击 IP”，可以展示对应被攻击 IP 的画像信息。



点击画像上的攻击源 IP 或诱捕器名称，可以钻取到对应攻击 IP 对指定诱捕

器实施攻击产生的风险事件和诱捕日志列表。

2.2.6 攻击者溯源

若攻击者访问诱捕器后被采集到攻击者特征信息，则攻击 IP 后会出现人像按钮，点击按钮则可以查看对应 IP 的溯源信息。

攻击者溯源信息：

2.2.1 诱捕器信息

在诱捕日志列表里点击诱捕器名称，可以查看到产生该诱捕日志的诱捕器详情：

诱捕器详情包括诱捕器基本信息、攻击画像、风险事件和诱捕日志信息。

3 策略

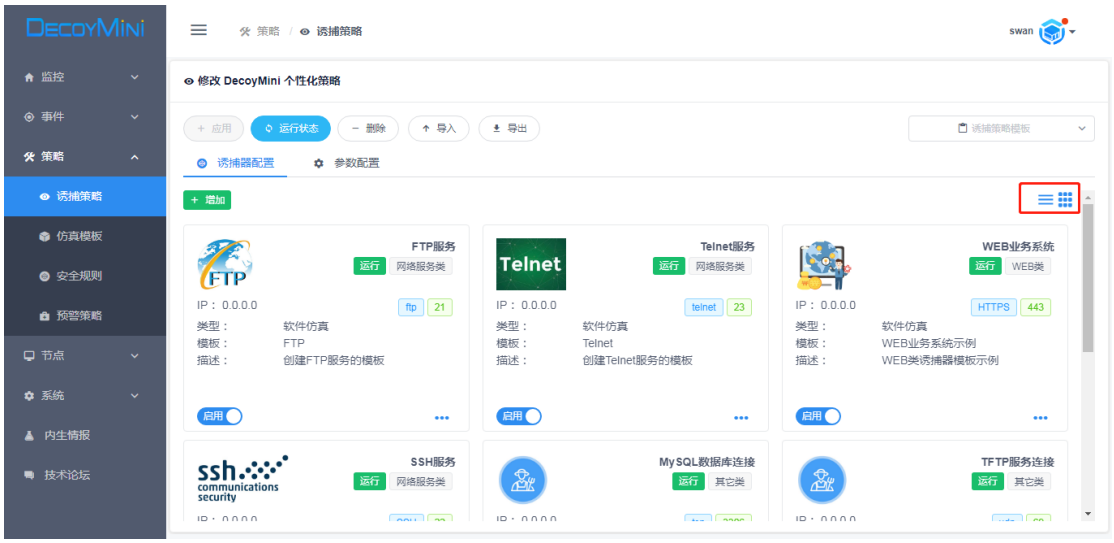
策略提供对诱捕策略、仿真模板、安全规则、预警策略等核心业务进行配置的功能。

3.1 诱捕策略

诱捕策略用于配置各诱捕探针需要执行的诱捕策略。

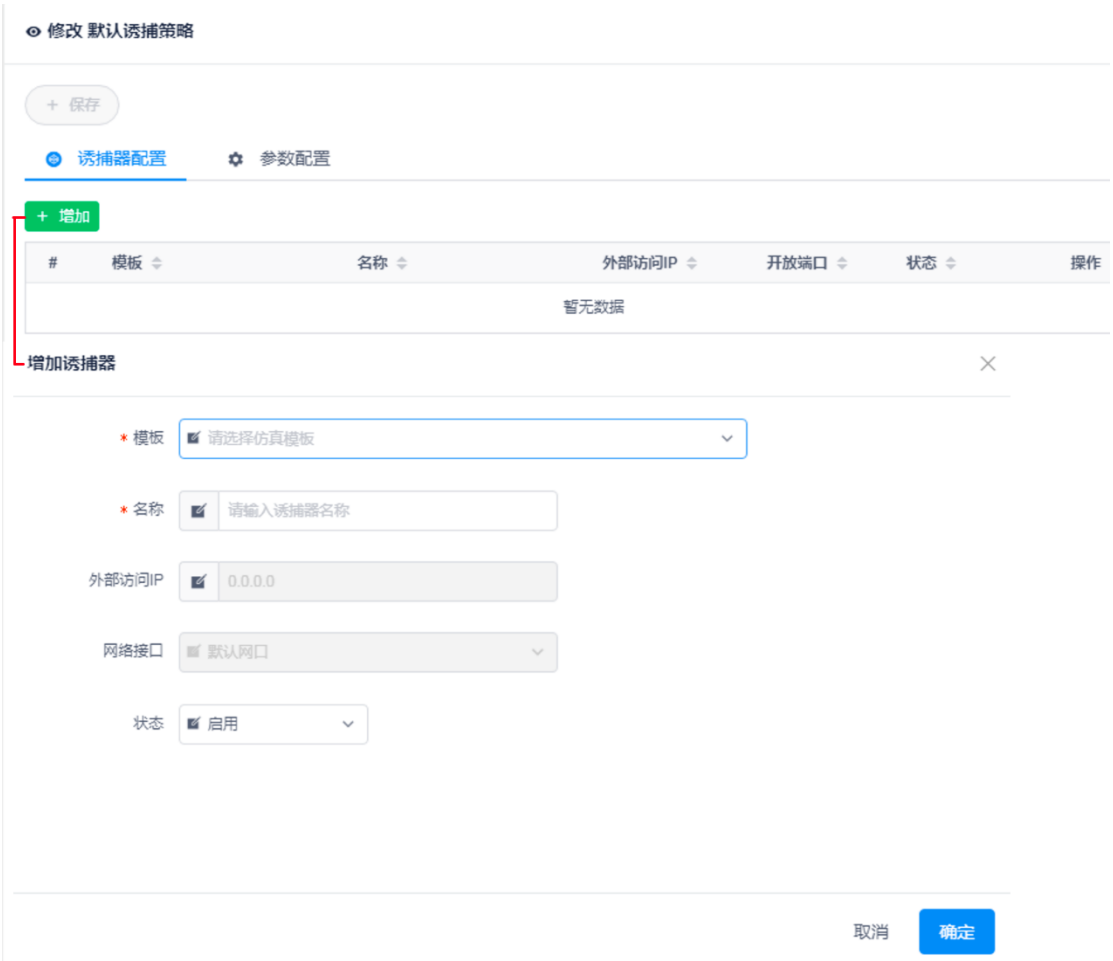
3.1.1 策略配置

诱捕策略支持“列表视图”和“卡片视图”展示方式，通过右上角图标可以进行切换。如下图所示：



DecoyMini 默认策略已添加了部分诱捕器，当各诱捕探针未配置个性化策略时，将会自动应用默认策略。同时，系统也内置了策略模板，通过选择策略模块可以快速导入对应策略模板的策略配置。

增加自定义诱捕策略，选择需要配置的诱捕探针，点击页面上的 "+增加" 按钮，可以增加诱捕器来为此诱捕探针定制个性化诱捕策略，如下图所示：



配置诱捕器相关参数：

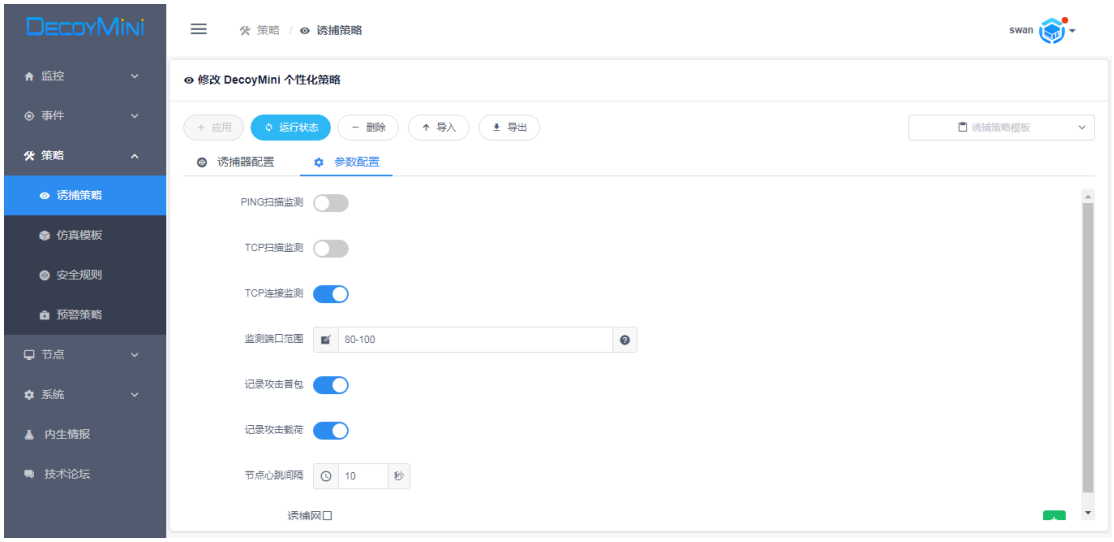
- 模板：诱捕器需要使用的仿真模板；
- 名称：诱捕器的名称；
- IP 地址：DecoyMini 支持虚拟 IP 技术，在增加新诱捕器时，诱捕器的外部访问 IP 支持填写网络可达范围内的空闲 IP，来将诱捕器直接部署在这个空闲 IP 上，比如网络里 192.168.1.8 这个 IP 还没有使用，用这个 IP 来部署一个 SSH 诱捕器，部署好后，攻击者通过网络扫描时就会扫描出 192.168.1.8 这个主机，扫描这个主机开放的端口就能看到 SSH 的 22 端口，通过这个 22 端口就能够连接到 SSH 蜜罐。通过虚拟 IP 技术可以用较少的资源来有效提高诱捕器的覆盖率，增加攻击者主动攻击蜜罐环境的概率；
- 协议：诱捕器运行的协议；
- 动态端口：监听的网络端口，支持配置指定端口(A)、端口列表(A,B,C)

或端口范围(A-B),配置了多个端口后诱捕器启动时会随机从端口中选取一个端口来运行诱捕器;

- 状态：启用状态;

说明：不同模板对应的配置参数会有差异，根据提示进行配置即可。当填写完成参数后，点击 "确定" 按钮保存威胁诱捕器配置。

“参数配置”标签页配置诱捕探针如下参数：



- PING 扫描监测：探针节点被 ping 时，产生诱捕日志;
- TCP 扫描监测：探针节点有 TCP 扫描时，产生诱捕日志;
- TCP 连接监测：探针节点有 TCP 连接时，产生诱捕日志;
- 监测端口范围：TCP 连接监测的端口范围，在启用 TCP 连接监测后有效，端口段用-（中划线）分割，多个端口用,（逗号）分割;
- 记录攻击首包:记录攻击连接第一个数据包,启用 TCP 连接监测后有效;
- 记录攻击载荷：记录攻击连接数据载荷，启用 TCP 连接监测后有效;
- 节点心跳间隔：探针节点与管理节点之间的心跳间隔，建议为 10 秒;
- 诱捕网口：配置探针节点诱捕器使用的网口，在使用多个网口来部署诱捕器的场景下有效;

当完成诱捕器及参数配置后，点击 "  " 按钮来应用此诱捕策略。

如果需要撤销最近的编辑操作，可以点击“  ”来将策略还原

到编辑前的状态。

3.1.2 运行状态

当诱捕策略应用后，在“列表视图”下通过 “运行”列可以查看诱捕策略的运行状态。

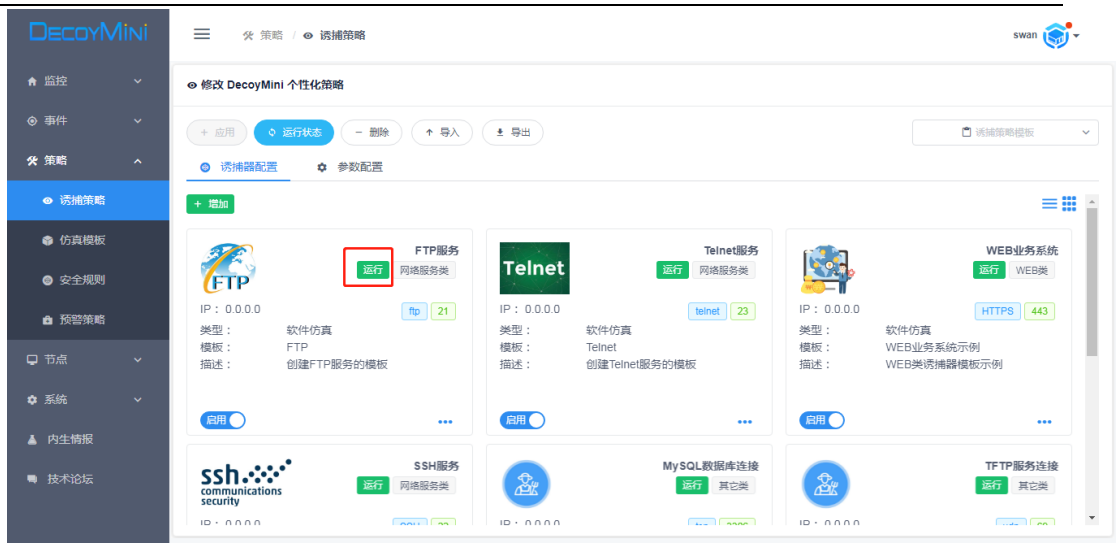
为正在运行

为运行失败，鼠标移动到图标上将会显示失败具体原因

为禁用状态

为策略待下发状态

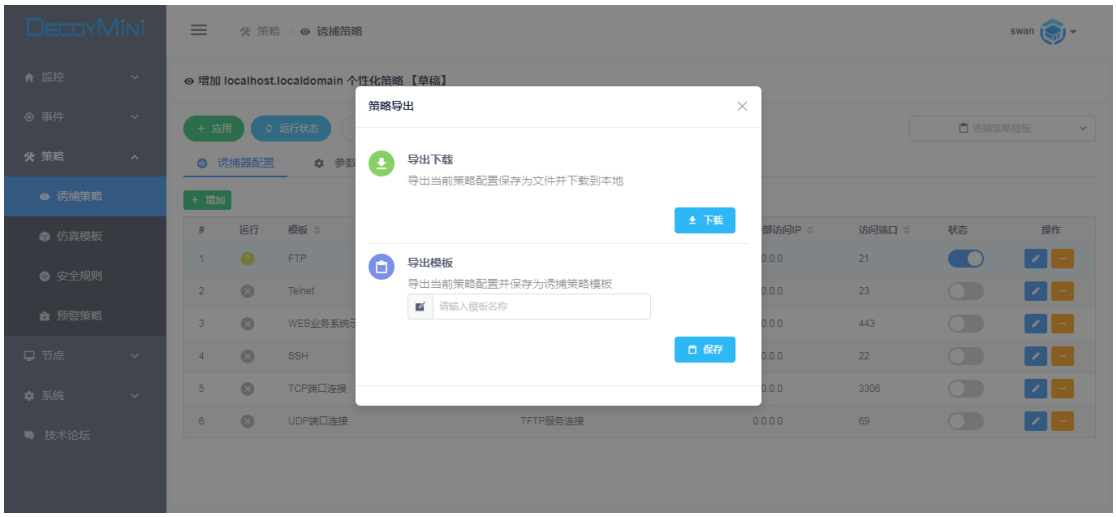
在“卡片视图”下，当诱捕器有绿色标签“运行”，则表示该诱捕器正在运行：



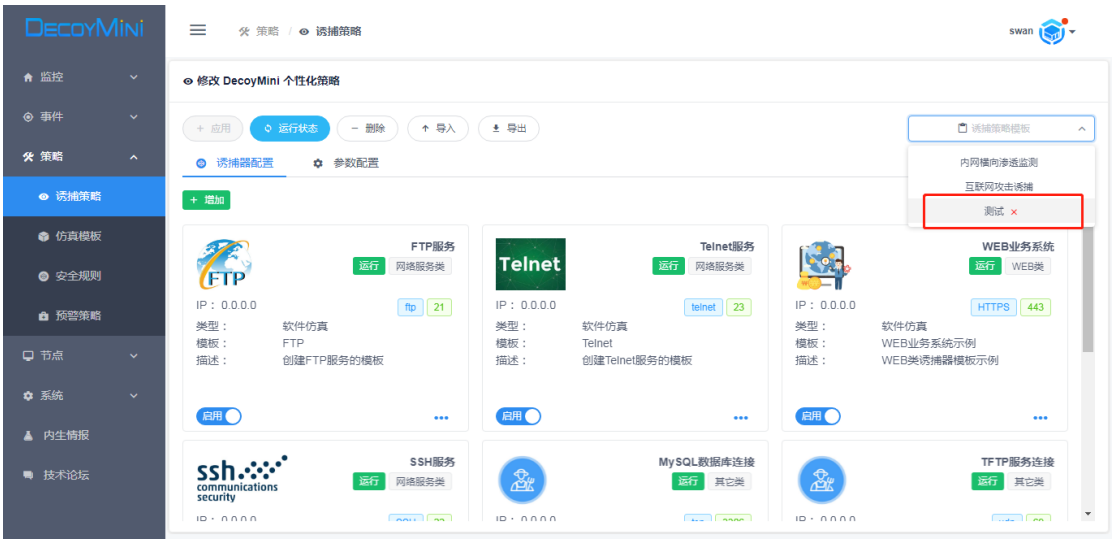
也可以点击“ 运行状态 ”查看诱捕器运行状态详情。

3.1.3 策略导出导入

点击“导出”按钮可以将当前选定的探针的诱捕策略导出下载到本地或者导出保存为模板；



导出策略为模板后，可以在右上角诱捕策略模板列表里选择该模板来加载对应策略数据到当前节点，点击模板名称后面的 × 可以删除该自定义模板。



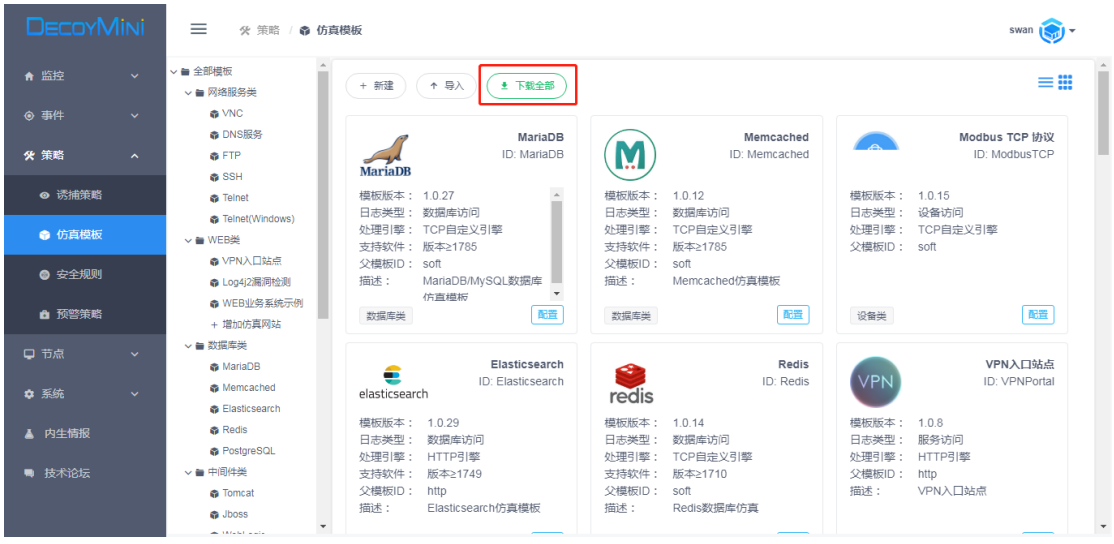
点击“导入”按钮，选择需要导入的策略文件，则可以将之前导出的策略文件导入到当前节点。

3.2 仿真模板

仿真模板提供对系统各仿真能力进行配置管理的功能，通过仿真模板可以快速、灵活自定义仿真内容。

3.2.1 模板管理

点击 "策略" --> "仿真模板"，可以打开仿真模板管理页面：



仿真模板默认按类别进行分类展示，系统默认包括如下分类：

- 网络服务类；
- WEB 类；
- 数据库类；

- 中间件类；
- 应用类；
- 设备类；
- 其它类；
- 基础模板；

在 DecoyMini 仿真模板列表界面提供模板一键下载功能，在能够连接互联网的环境，使用论坛账户登录后，点击“下载全部”按钮，可以一键自动下载论坛里常用仿真模板集合。

选择需要配置的模板，则进入模板对应的配置操作界面，如下图所示：

模板配置界面提供对基础信息、参数配置、响应数据、资源文件、作者信息等进行配置的功能。

- 基础信息：定义该仿真模板的基本信息；
- 参数配置：定义该模板的配置参数；
- 响应数据：定义模板响应数据；
- 资源文件：定义模板运行所需的资源文件；
- 作者信息：填写模板的作者信息；

通过对仿真模板的自定义配置，可以灵活自定义仿真内容，灵活配置对网络请求数据的各种解析方式和定义应答数据，实现灵活扩展仿真能力和对新的网络协议或服务的仿真。详细内容介绍参见“自定义模板”章节。

3.2.2 模板下载

在能够连接互联网的环境，系统支持自动访问论坛同步最新的仿真模板列表，对本地还未导入的模板，通过界面可实现一键下载导入。

在左侧仿真模板树形列表中，模板名称后有绿色下载图标的，表示该模板本地尚未导入，可以点击打开后单击“下载模板”来下载导入此模板；同时也可以点击模板信息下方的“论坛地址”访问论坛来查看该模板的详细信息。

对于不能连接互联网的环境，可以在论坛里手动下载模板导入到系统里使用。

3.2.3 模板升级

在能够连接互联网的环境，针对本地已经导入的模板论坛里有更新的，支持通过管理端界面一键将模板升级到最新版本。

在左侧仿真模板树形列表中，模板名称后有橙色升级图标的，表示该模板有更新的版本。

点击模板操作区的“模板升级”按钮，进入模板下载升级页面，点击“下载模板”可以将本地模板升级到最新版本。

对于不能连接互联网的环境，可以在论坛里手动下载更新的模板导入到系统里进行升级。

3.2.4 增加仿真网站

系统支持自动仿真用户自定义网站的能力，通过系统内置的网页爬虫对指定目标网站进行自动爬取可以快速生成对应网站的 WEB 仿真模板。利用此功能，可以将用户自己的一些业务系统站点快速生成仿真模板，并通过诱捕器部署出来，这样在安全监测、攻防演习等实战场景下对攻击的诱捕效果更佳。

在左侧仿真模板树形列表中点击“ + 增加仿真网站 ”，可打开增加仿真网站

配置界面：

在模板配置中配置对应参数：

- 模板 ID：模板的唯一标识；
- 模板名称：模板的显示名称；
- 仿真目标网站地址：要仿真的目标网站地址，支持 http 和 https；例如：https://www.taobao.com
- 网站数据同步周期： 在 WEB 仿真模板生成后，系统支持定期自动更新模板里的仿真页面内容。0 为不自动更新；>0（单位：天)则表示每间隔指定天数自动更新；
- 描述：对模板的描述信息；

当完成参数配置，点击“增加”按钮后稍等片刻，就完成增加对自定义网站的 WEB 仿真模板。

3.3 自定义模板

对于私有协议和自定义仿真需求，可以基于系统仿真模板配置界面来自定义新的仿真模板或对现有仿真模板进行定制化。系统内置了一个可视化仿真编排引擎，通过界面自定义对请求数据的解析规则，提取出关键属性，基于对关键属性的判断，来响应对应的个性化数据，进而实现对协议或服务的仿真。基于仿真模板配置框架，可以配置具备中、高交互能力的威胁诱捕器。

可以访问如下链接查看利用 DecoyMini 来自定义仿真模板的实例：

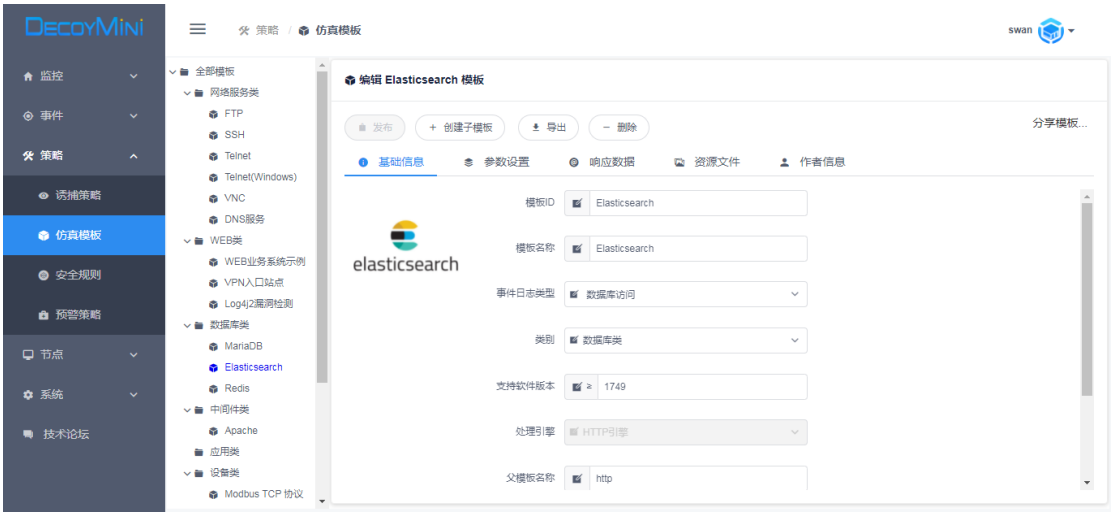
- 用免费蜜罐软件快速部署业务系统蜜罐：
  - https://www.freebuf.com/articles/es/328397.html
- 用免费蜜罐工具配置 Modbus 工控蜜罐：
  - https://www.4hou.com/posts/lXB7

对于自定义的模板，可以导出并分享到技术论坛，对分享了仿真模板的会员，论坛会给予礼品或现金奖励。

3.3.1 基础信息

基础信息配置为配置该仿真模板的基本参数，包括定义该仿真模板的 ID、

名称、事件日志类型、类别、处理引擎、父模板名称、运行环境、版本、描述等信息；界面如下图所示：



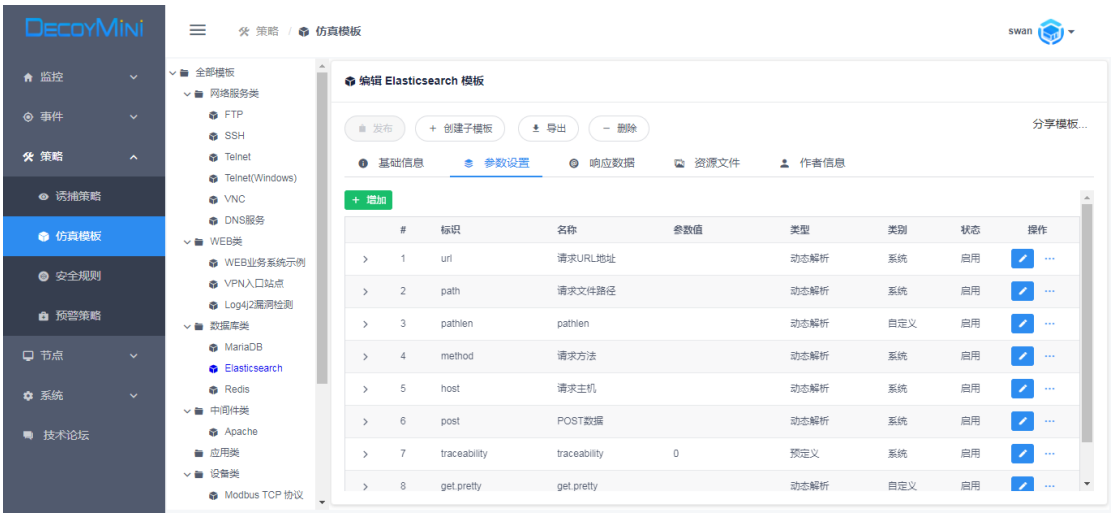
主要参数说明如下：

- 模板 ID：模板唯一标识，创建后不可修改
- 模板名称：模板展示名称（支持中文）
- 事件日志类型：对应诱捕日志中显示的日志类型
- 类别：仿真模板的类别，主要用于模板分类显示
- 支持软件版本：仿真模板运行需要的最低软件版本号（版本序列号）
- 处理引擎：模板处理的引擎，不可修改
- 父模板名称：模板对应的父模板 ID，不可修改
- 模板版本：模板版本号，不可修改，每次发布版本号会自动增加
- 描述：模板描述信息

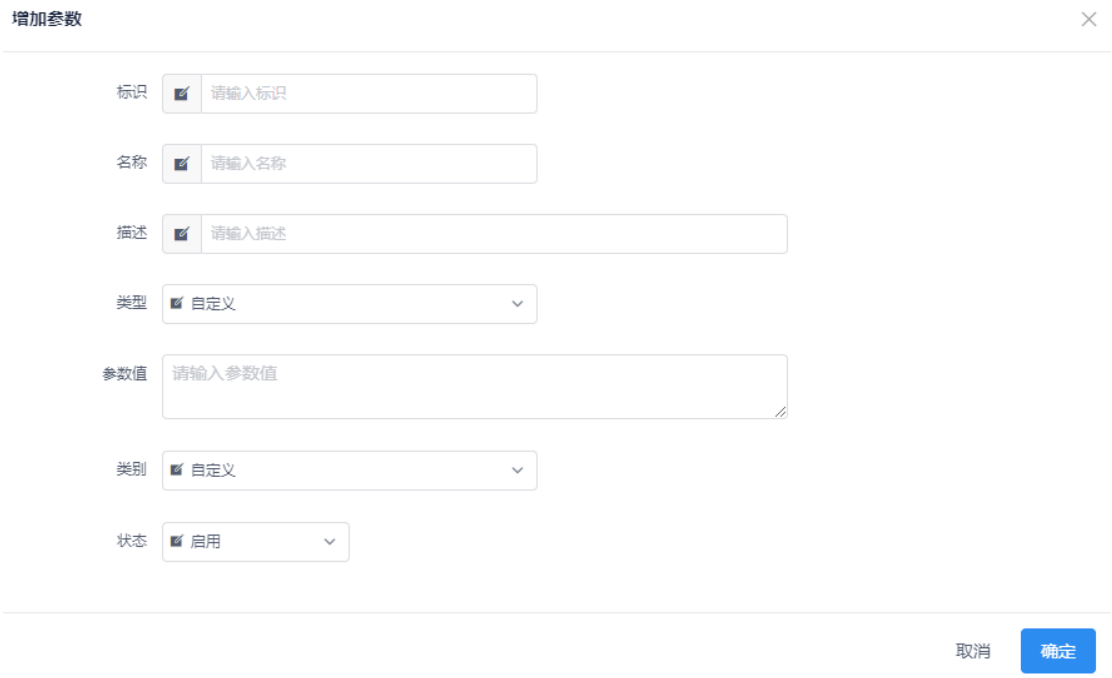
3.3.2 参数配置

1. 基本配置说明

参数配置用于配置模板运行所需的参数，配置的参数可以在响应数据里引用。界面如下图所示：



点击增加按钮，可以增加配置参数。界面如下图所示：

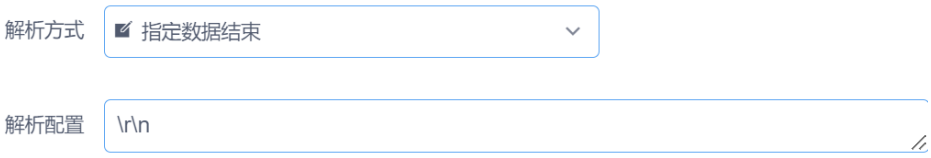


配置的属性说明如下：

- 标识：参数标识，仅支持数字、字母、下划线
- 名称：参数展示名称（支持中文）
- 类型：参数的类型，可以为：
  - 动态解析：根据网络请求数据按照指定的规则进行解析；
  - 预定义：引擎预定义的参数；
  - 自定义：用户自定义参数；
- 解析方式：类型为“动态解析”时，配置对参数的解析方式

- 自动解析：引擎自动解析参数值
- 规则解析：配置解析规则来解析参数值

- 数据源：采用“规则解析”时，解析的数据来源；
  - 网络请求数据：直接解析网络请求数据
  - 缓存数据：解析已缓存的数据（缓存数据在“解析选项”的“缓存最新数据”里配置）
- 缓存数据：选用“规则解析”/“缓存数据”时，选择需要解析的缓存数据名称；
- 解析方式（选择“网络请求数据”项时）
  - 指定数据结束：读取到特定数据结束读取（例如：\r\n）



- ✓ 字符：直接输入
- ✓ 十六进制：输入 “\xXX”(XX 必须两个字符,\x0a)

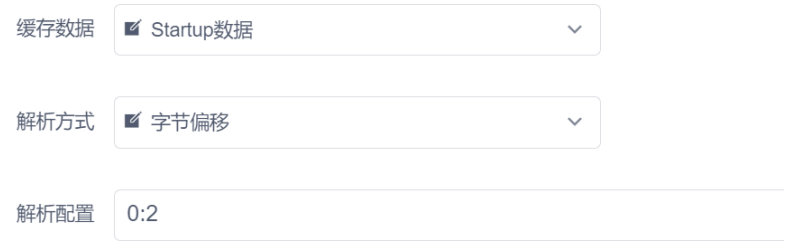
说明：参数保存时不包含配置的结束符

- 指定长度：读取到特定长度结束读取

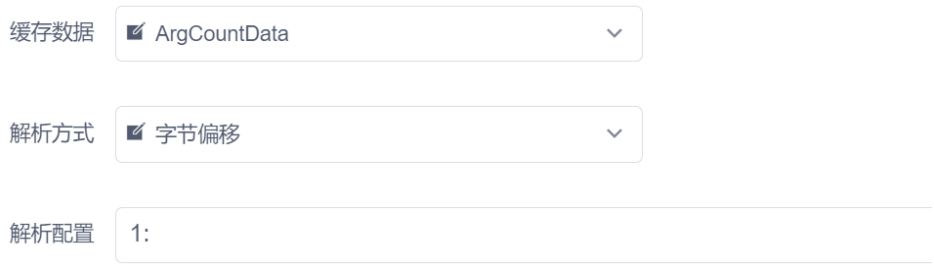
- ✓ 数字：直接输入数字字符串
- ✓ 变量：输入变量{{argName}}
- ✓ 运算符：支持加减乘除

- 解析方式（选择“缓存数据”项时）
  - 字节偏移：以字节为单位截取数据，格式 nStart:nEnd，索引从 0 开始，包含索引 nStart 字符，不包含索引 nEnd 字符，nEnd 最大为数组大小，nEnd 不填则自动设置为数组大小
    - ✓ 数字：直接输入数字字符串
    - ✓ 变量：输入变量{{argName}}
    - ✓ 运算符：支持加减乘除

    例如：截取前两个字节：

    例如：截取第一个字节后的数据：

    例如：偏移位置支持变量及运算：

- 位偏移：以位为单位截取数据，格式 nStart:nEnd，索引从 0 开始，包含索引 nStart 位，不包含索引 nEnd 位，nEnd 最大为位总长度，nEnd 不填则自动设置为位总长度

  例如：二进制 11001100 11001100 截取 3:13，二进制截取结果：01100110 01000000

  说明：位长度不是 8 的整数倍时，右侧自动补 0 至一个字节
- 正则分割：使用正则表达式将缓存数据切割成数组保存
- 字符串分割：使用字符串将缓存数据切割成数组保存

- 解析配置：配置的解析数据参数
- 数据类型：数据保存类型，支持字符串、字节数组、整数（大端）、整数（小端）
  - 字符串：原始字节数组对应的字符串
  - 字节数据：原始字节数组
  - 整数(大端)：按照大端方式转换为整数
  - 整数(小端)：按照小端方式转换为整数
- 解析操作：对数据的解析处理方法

- 正则替换：使用正则替换方式处理数据
  - ✓ 参数：正则表达式
  - ✓ 值：正则匹配的替换内容

- 字节替换：
  - ✓ 参数：需要替换的十六进制字符串
  - ✓ 值：替换内容的十六进制字符串
- Map 转换(字符分割)：仅支持缓存数据的正则、字符串分割，数组每行使用字符切割成 key value

  例如：

  原始字符串：usr=test,password=123456

  字符串分割(分隔符,)解析结果：

  usr=test

  password=123456

  Map 转换 (分隔符=)解析结果：

  key=usr; value=test

  key=password; value=123456

- Map 转换(换行分割)：仅支持缓存数据的正则、字符串分割，每两行对应一个 key value

  例如：原始字符串：usr0x00test0x00password0x00123456

  字符串分割(分隔符\x00)解析结果：

  usr

  test

  password

  123456

  Map 转换(换行分割)解析结果：

  key=usr; value=test

  key=password; value=123456

- 解析选项，支持多选：
  - 缓存最新数据：缓存数据可被二次解析

- 缓存历史数据：将相同参数追加到列表中直至清理参数
- 去除首尾空格：保存数据时去除首尾的空格、0x00 字符

- 超时时间：等待读取数据时间，0 为一直等待
- 参数值：预定义或自定义参数的参数值
- 类别：参数的类别
  - 系统：系统预定义参数
  - 自定义：用户自定义添加
- 描述：参数描述信息
- 状态：启用、禁用当前参数

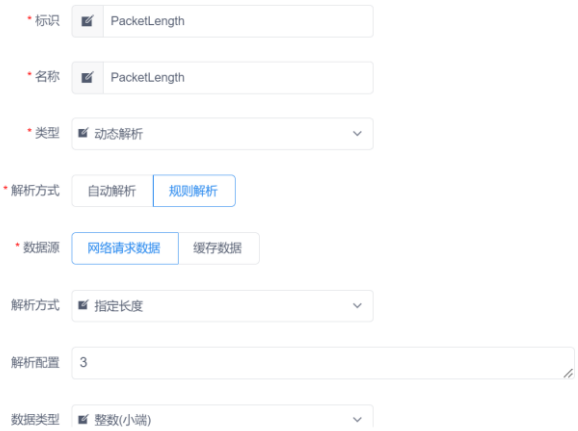
点击参数操作列的 "修改" 按钮，可以修改参数属性；

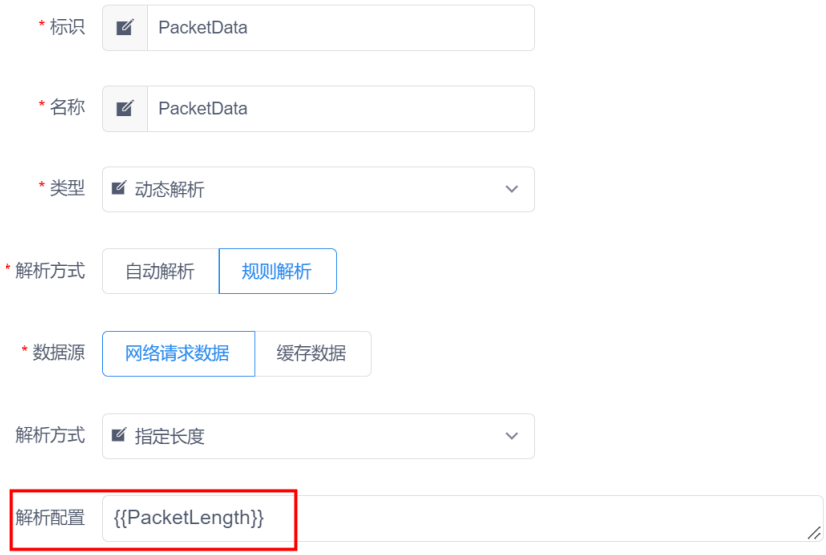
点击参数操作列的 "删除" 按钮，可以删除对应参数。

2. 参数引用格式：{{argName}}

1、采用 Mustache 语法{{argName}}格式获取 argName 参数的值，若参数值为数组或对象时，按 JSON 格式返回；

示例：引用上一次获取的长度信息（摘自 MariaDB 模板）

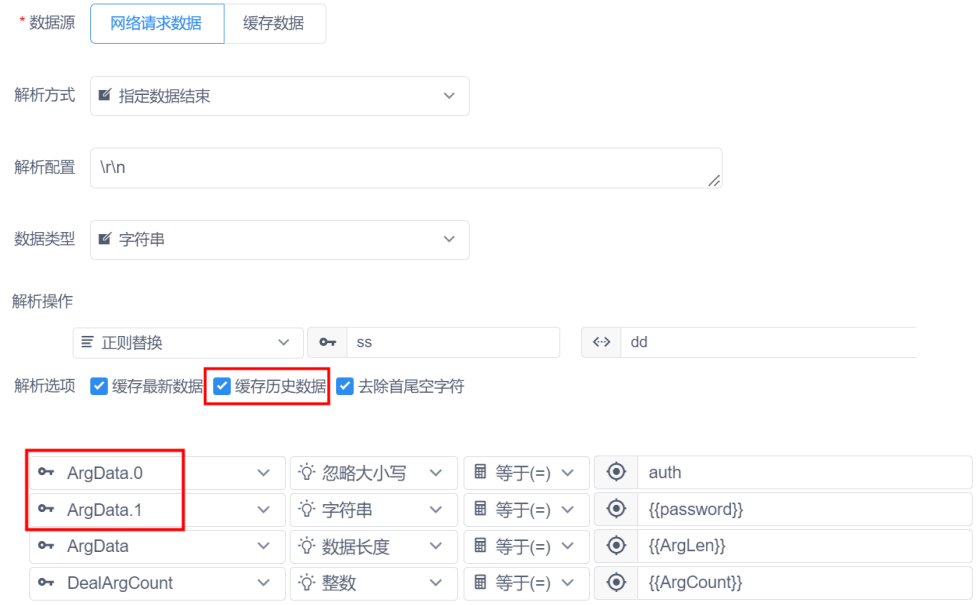




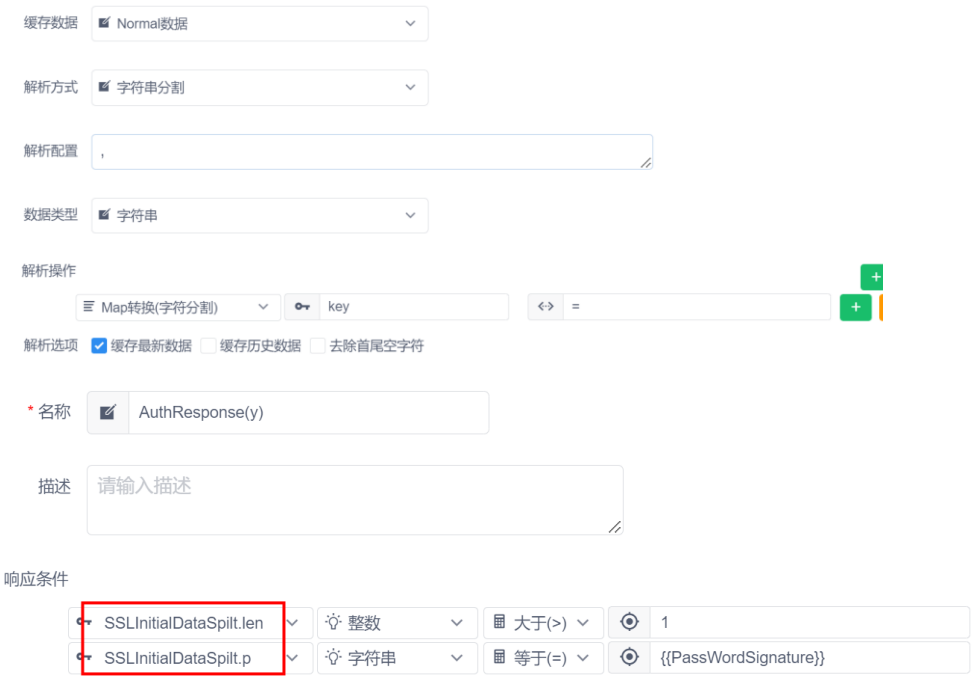
2、采用 {{argName.n}}格式来获取数组参数 argName 下标为 n 对应的值，n 为负数时，表示从右边开始计算；

3、采用{{argName.key}}格式来获取对象参数 argName 键名为 key 对应的值；

示例：数组序号查找（摘自 Redis 模板）



示例：切割 Map 后查找（摘自 PostgreSQL 模板）



3. 数组、对象大小：{{argName.len}}

数组：勾选“缓存历史数据”后每次都会追加数据到参数中，同时更新 argName.len 大小信息

对象：仅“正则分割”、“字符串分割”的参数支持将数组转换为对象访问，同时更新 argName.len 大小信息

4. 函数引用格式：{{funName(arg1,arg2)}}

1） 数组连接（仅数组参数支持）

{{join(argName, str)}}

例如：Reids 模板日志输出

参数 ArgData 数组值：SET runoobkey redis

连接字符串：空格" "

执行结果：SET runoobkey redis

2） 数值加/减

{{Add(argName,nStr)}}

输出二进制长度与第一个参数长度相同，减填负数。

示例：引用上一次获取的长度信息（摘自 MariaDB 模板）

5. 参数解析顺序说明

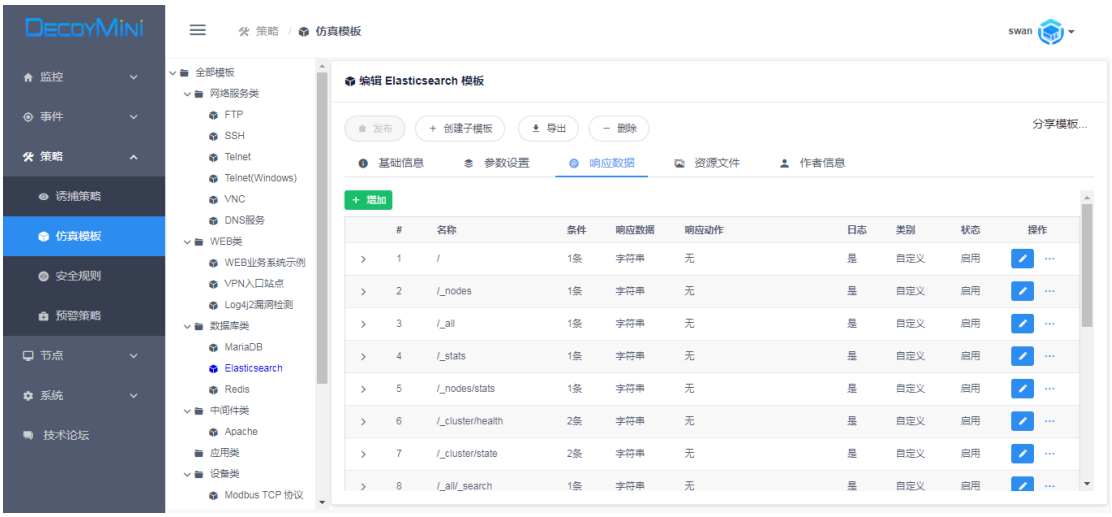
配置了多条参数时，解析时从序号由小到大顺序执行。

响应数据匹配成功，存在执行动作将执行相关动作；无响应数据执行动作，继续执行下一个参数解析操作；最后一个参数解析后无操作将断开连接。

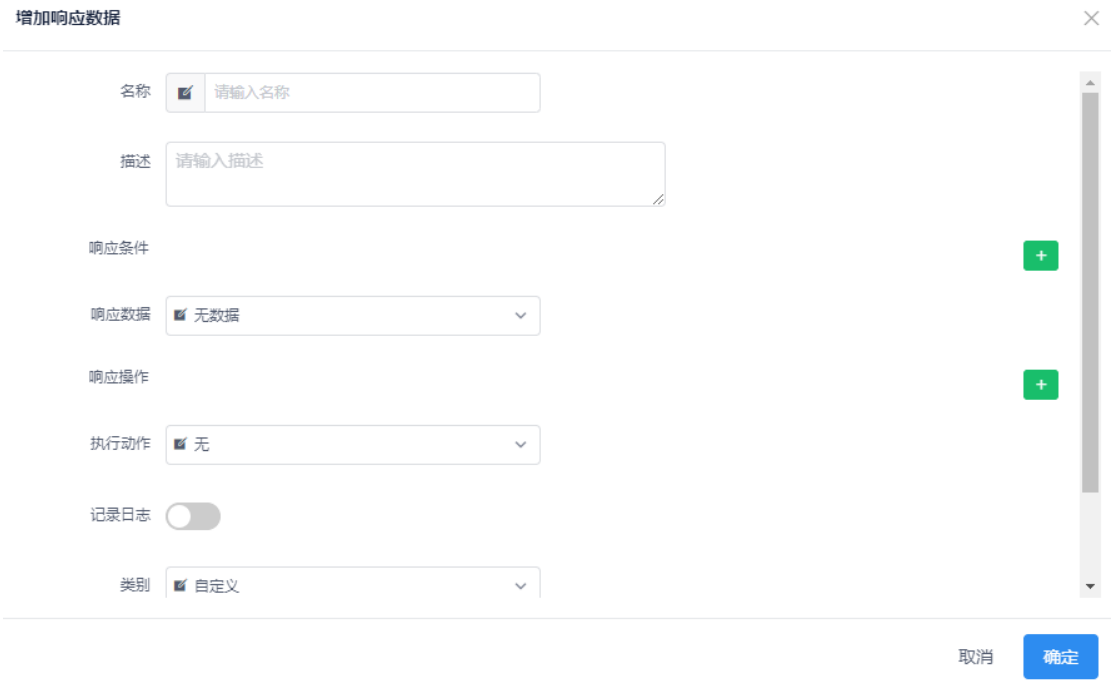
3.3.3 响应数据

1. 基本配置说明

根据请求参数配置对应的响应数据，如下图所示：



点击增加，可以增加一个响应数据，界面如下图所示：



对应的配置项主要包括：

- 名称：响应数据名称（支持中文）

- 描述：描述信息
- 响应条件：满足匹配条件后将响应本条响应数据
  - ✓ 多个条件是与(&)关系，必须同时满足
  - ✓ 执行顺序从上到下，遇到不满足的跳出判断（将最容易判断的条件放第一条可用加快运行速度）
  - ✓ 支持函数、参数引用、加减乘除运算、指定字符（如\r \n）及二进制数据（\xXX）

  - ✓ 或(|)条件采用配置多条响应数据来实现

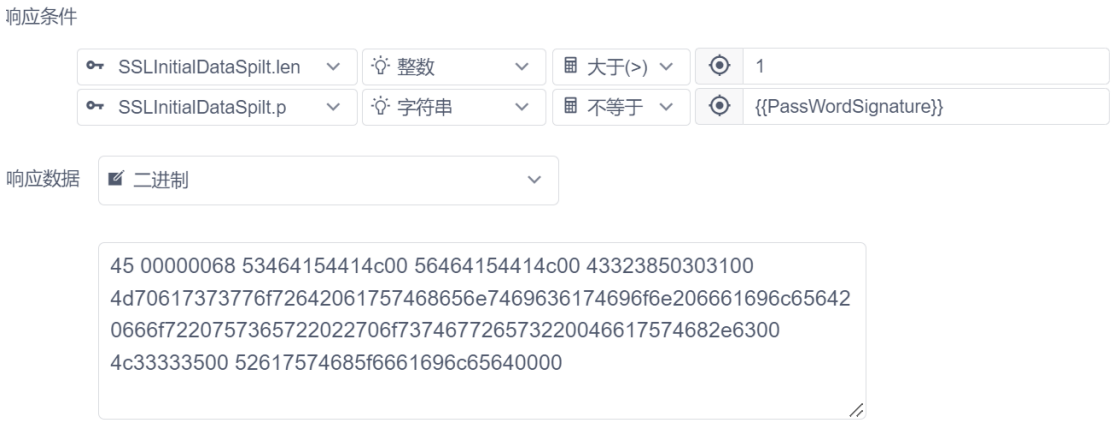
- 响应数据：返回的数据信息
  - ➢ 无数据：不响应任何数据；
  - ➢ 字符串：响应指定的字符串；

  - ➢ 二进制：响应二进制数据；

    将响应数据转为十六进制，忽略空格、空格视为分隔符

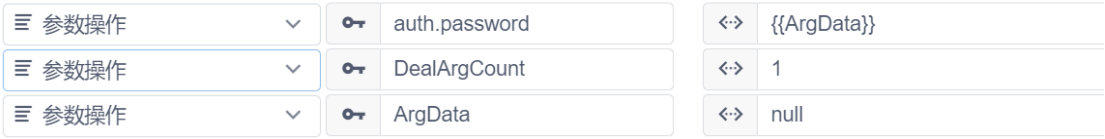
    例如：01aa02bb 对应的二进制为： 0x01 aa 02 bb

    1 aa 2 bb 对应的二进制为： 0x01 aa 02 bb

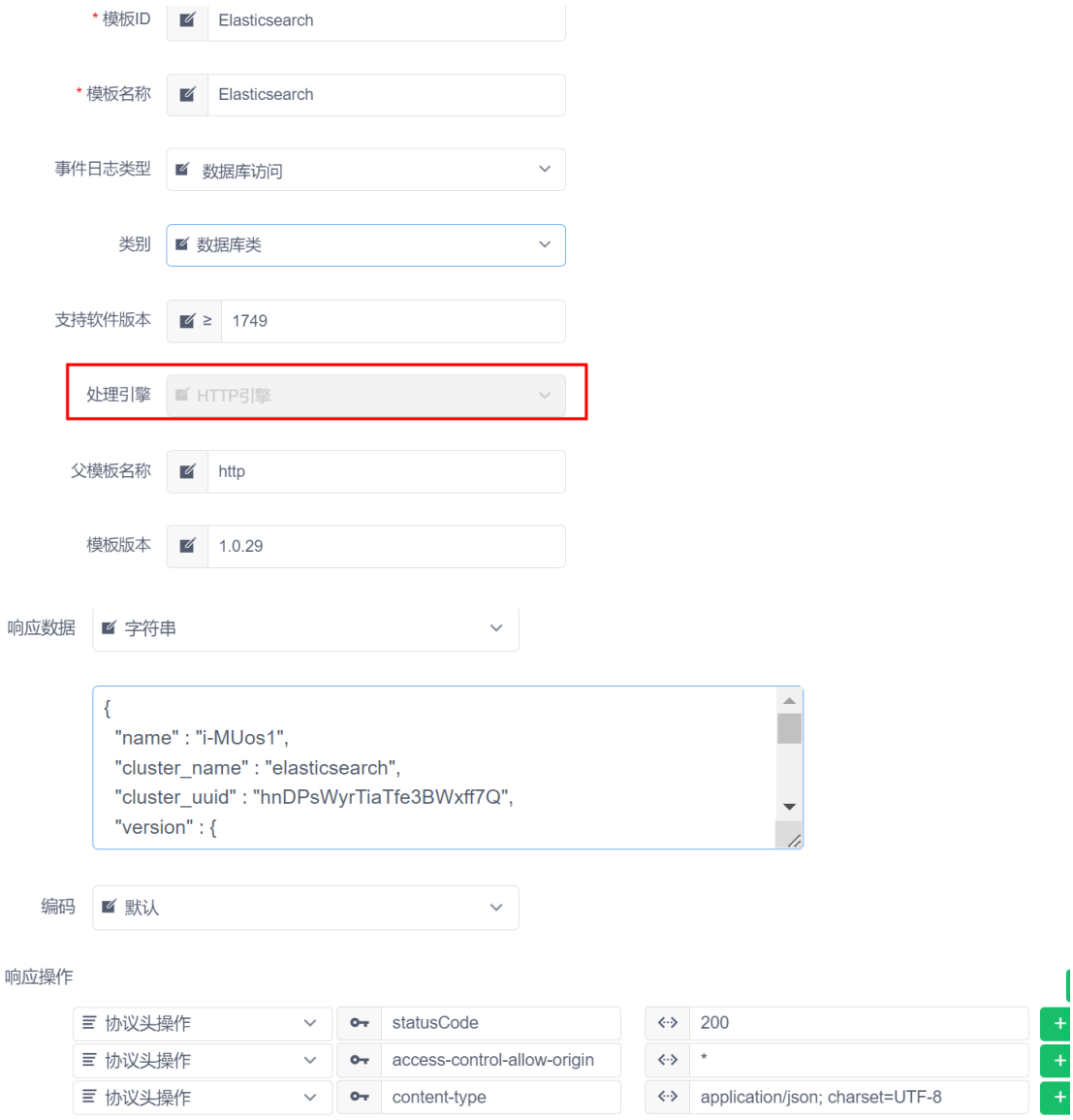


- 数据文件：响应资源文件里“数据文件”目录下指定文件内容；
- 配置文件：响应资源文件里“配置文件”目录下指定文件内容；
- 文件系统：响应资源文件里“文件系统”目录下指定文件内容；

- 响应操作：响应同时执行相应的操作
  - 参数操作：对参数进行操作
    - ✓ 支持函数、参数引用、加减乘除运算、指定字符（如\r \n）及二进制数据（\xXX）
    - ✓ 原始值是字节数组时，系统自动将字符串值转换字节数组
    - ✓ 参数值赋予 null，表示清理相关参数



  - 协议头操作：对 HTTP 协议头进行操作，仅支持 HTTP 引擎
    - ✓ 示例：返回数据前增加协议头信息



- 执行动作：响应执行完毕后是否执行特殊动作
  - 无：不执行特殊动作；
  - 新会话：开启新会话；
  - 结束会话：结束当前会话；
  - 跳转到参数：跳转到指定参数继续执行；
- 记录日志：响应数据后是否启用输出日志记录；
- 记录条件：输出日志的条件（多个条件间为与关系）
- 操作用户：对应诱捕日志中的用户信息
- 操作类型：对应诱捕日志中的动作信息
- 操作结果：对应诱捕日志中的操作结果，可以配置为成功或失败
- 日志描述：对应诱捕日志中的描述信息

- 日志级别：对应诱捕日志中的日志级别
- 记录参数：对应诱捕日志详情中看到的附加参数信息
- 类别：系统、自定义
- 状态：启用、禁用

点击 "编辑" 按钮，则可以编译对应的响应数据项；

点击 "删除" 按钮，可以删除对应的相应数据。

2. 响应数据执行说明

连接建立成功后，查找是否存在名称为"_init"的响应数据，有则先执行此响应数据，然后从响应数据序号由小到大顺序执行。

在匹配响应条件时，如果有一条不满足则跳出继续后继响应数据匹配。

当响应条件匹配成功后，执行响应操作，执行的先后顺序如下：

1. 查找是否存在类别为“系统”，名称为“argName.prefix”的预定义响应数据，如果存在则执行此响应数据；
2. 返回当前响应数据；
3. 查找是否存在类型为“系统”，名称为“argName.suffix”的预定义响应数据，如果存在则执行此响应数据；
4. 执行响应操作；
5. 执行日志上报；

6. 执行参数清理；
7. 执行跳转动作。

3. 响应数据的循环处理

响应数据的循环处理配置示例如下：

1、自定义循环处理次数参数：默认配置为 1

2、勾选“缓存历史数据”，每次解析到新数据后都会追加数据到参数中，同时更新 argName.len 大小信息

3、增加循环响应操作：

- 响应条件
  - ✓ 本次参数读取完成：ArgData 长度 等于 {{ArgLen}}

- ✓ 已处理参数数量小于参数数量 DealArgCount 小于 {{ArgCount}}

➢ 响应数据：无

➢ 响应操作：DealArgCount+=1

➢ 执行动作：继续执行循环开始 ArgLenData

4、循环完成重置相关参数：

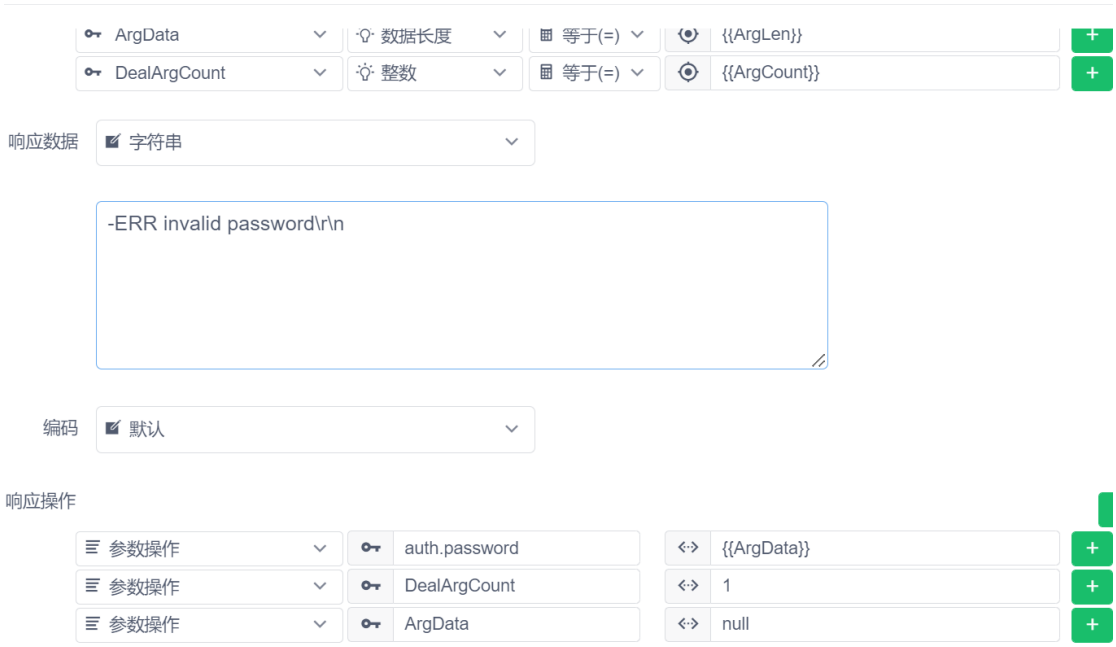
➢ 响应条件

- ✓ 数据处理完成：ArgData 长度 等于 {{ArgLen}}
- ✓ 已处理参数数量等于参数数量 DealArgCount 等于 {{ArgCount}}

➢ 响应数据：字符串

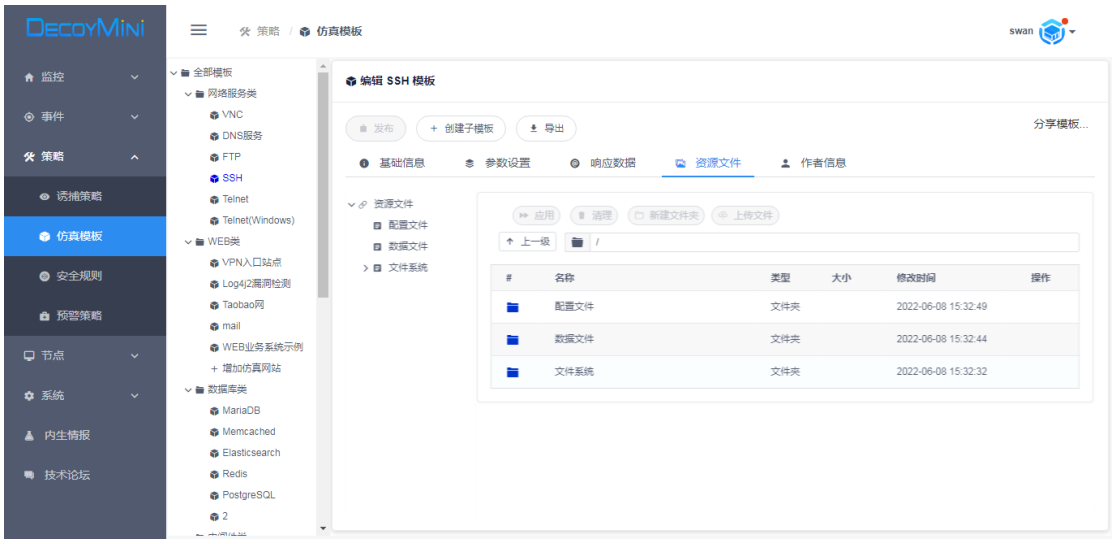
➢ 响应操作：

- ✓ 设置记录参数：auth.password
- ✓ 重置 DealArgCount：DealArgCount 值 1
- ✓ 清理参数 ArgData：ArgData 值 null，一次循环完成需要清理参数，否则会一直追加导致异常
- ✓ 执行动作：继续执行数据开始 ArgCountData



3.3.4 资源文件

资源文件功能用于配置仿真引擎和响应数据所需的资源数据和文件。界面如下图所示：



资源文件系统默认目录及文件说明如下：

- 配置文件：存放模板运行所需的配置信息；
  - logo.png：模板展示的图标
  - server.crt：模板使用的证书文件（HTTP、FTP、HTTP 智能引擎有效）
  - server.key：模板使用的私钥文件（HTTP、FTP、HTTP 智能引擎有效）

- id_rsa：模板使用的证书信息（SSH 引擎有效）

- 数据文件：存放模板所需的数据文件；
- 文件系统：存放仿真文件系统数据；

选择一个资源文件类别，点击 "新建文件夹"，可以创建一个新的文件夹；点击 "上传文件"，可以将本地的文件上传到当前的资源目录下。

完成资源文件编辑操作后，点击“ 应用 ”按钮可以将更新的资源文件应用到诱捕器上。

点击“ 清理 ”” 按钮，可以撤销从上次应用后所做的临时修改。

3.3.5 作者信息

用于设置编写此仿真模板的作者信息，方便在仿真模板分享、使用过程中与作者进行联系。

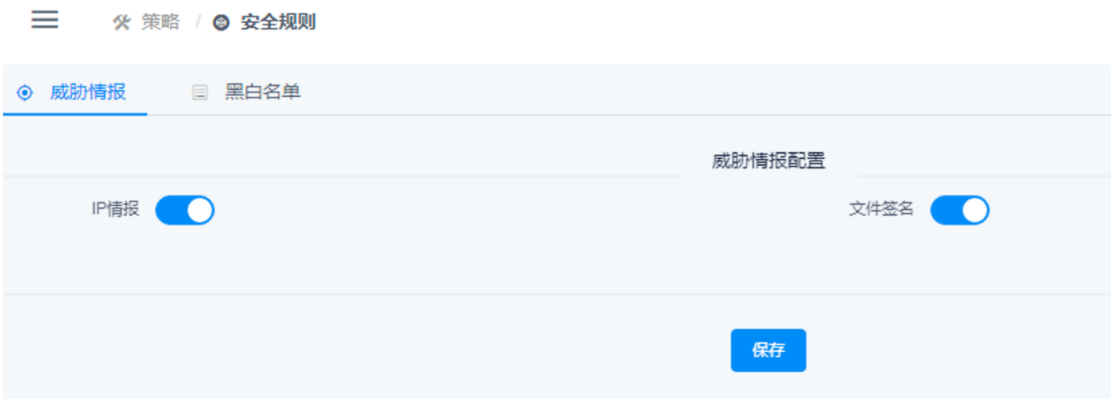
3.4 安全规则

安全规则用于配置系统安全监测规则，包括威胁情报配置和黑白名单配置等。

3.4.1 威胁情报

系统支持威胁情报检测能力，通过定期和云端威胁情报平台同步，及时更新最新的情报数据到本地，利用威胁情报能够快速发现恶意 IP 和恶意文件等。点击 "策略" --> "安全规则" --> "威胁情报" 标签，可以打开威胁情报配置页面，

如下图所示：

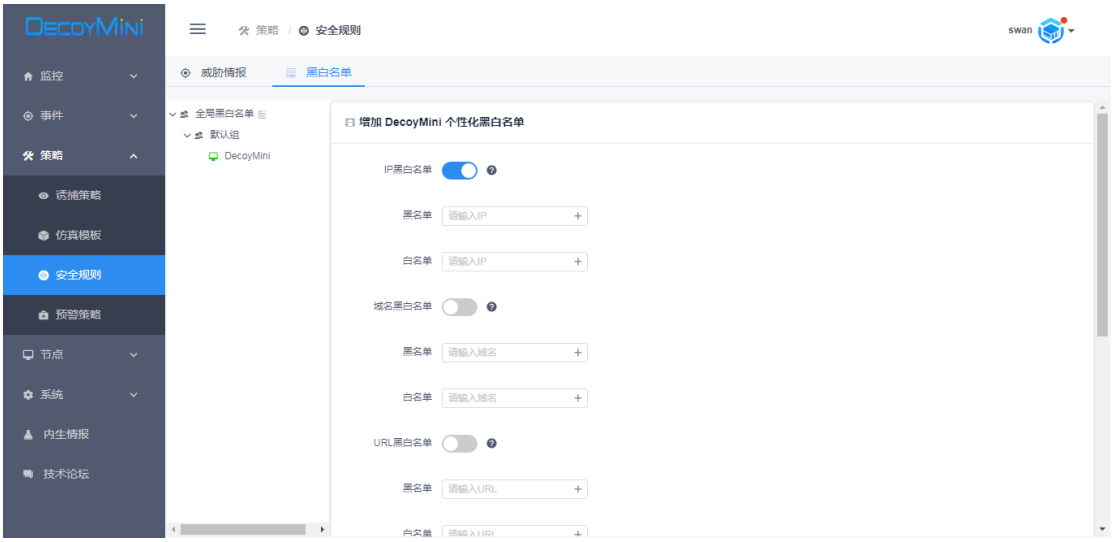


3.4.2 黑白名单

黑白名单功能用于配置黑白名单，系统支持配置各类白名单，添加到白名单的数据将不做告警；支持按需配置黑名单，匹配到黑名单里的日志将进行告警。系统当前支持的黑白名单种类如下：

- 文件黑白名单；
- IP 黑白名单；
- 域名黑白名单；
- URL 黑白名单；
- 端口黑白名单；

点击 "策略" --> "安全规则" --> "黑白名单" 标签，可以打开黑白名单配置页面，如下图所示：



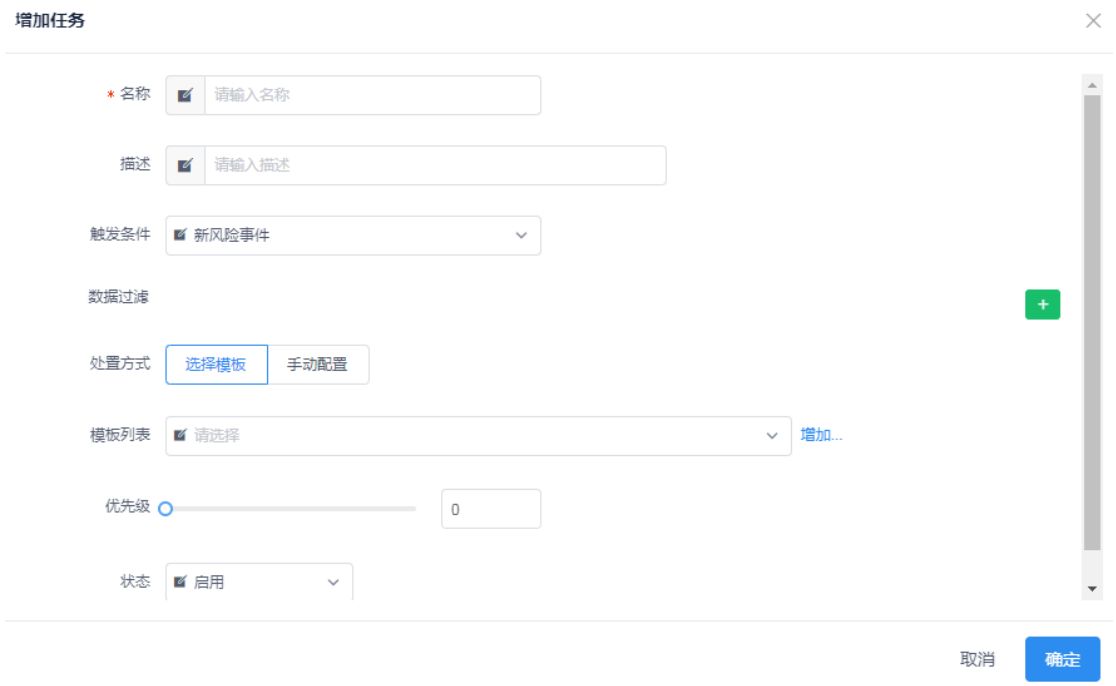
选择需要应用的节点，配置对应的黑白名单，点击 "保存" 按钮，即可保存

应用黑白名单配置。

3.5 事件预警

当产生了特定的风险事件后，支持通过多种方式发送事件预警通知。包括邮件告警、弹窗告警、企业微信，钉钉、飞信、Syslog 输出等方式。

在预警策略界面点击“增加”按钮增加预警任务，界面如下所示：



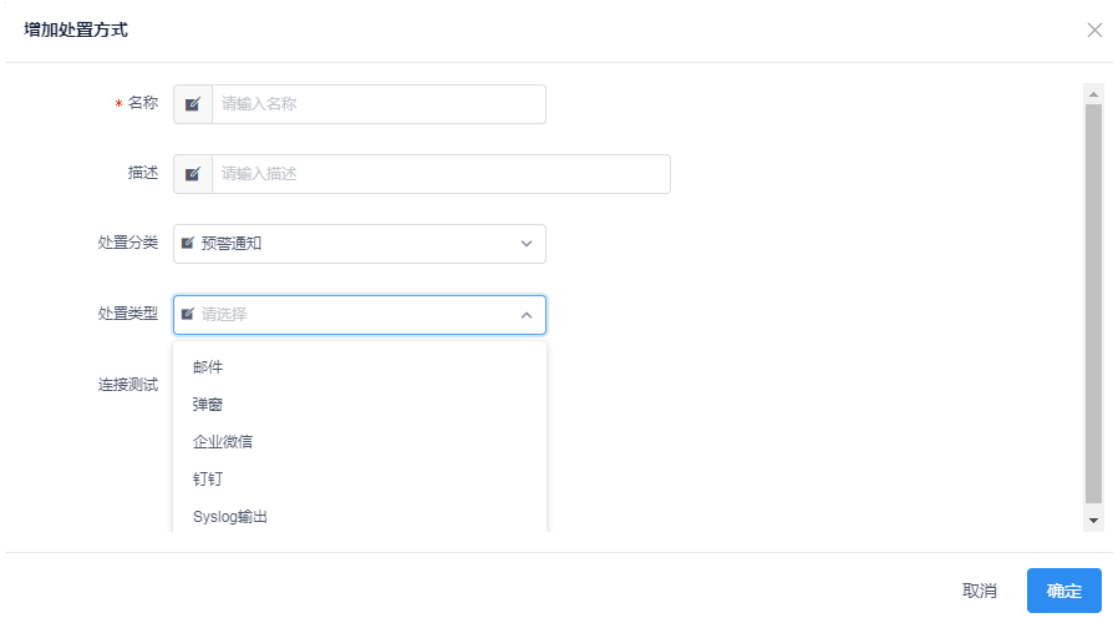
依次填写预警参数，主要参数说明如下：

- 名称：任务的名称；
- 描述：任务描述信息；
- 触发条件：默认选择当产生新风险事件后触发任务；
- 数据过滤：配置过滤条件，未配置过滤条件或者配置的多个条件同时都满足后，才会执行后继预警处置任务；
- 处置方式：配置预警处置方式，支持“手动配置”和“选择模板”两种方式，可以提前配置好处置方式模板，方便后继预警策略直接选择该模板来引用；
- 优先级：任务执行的优先级，值越大最先执行；
- 状态：任务的启用状态。

当保存事件预警任务配置后，系统产生符合条件的风险事件时就会通过配置

的方式自动进行预警。

在预警策略界面，点击“处置方式”标签，可以预先配置好处置方式模板，方便后继处置任务的配置。处置方式配置界面如下所示：



3.5.1 企业微信接入

1、添加群机器人

桌面客户端：右键需添加机器人的群，点击 “管理聊天信息” -> ”“添加群机器人”，填写机器人名称点击完成即可添加成功。

手机端： 进入需添加群机器人的群聊，点击右上角的图标进入聊天信息页面，点击“群机器人”即可添加。

2、使用群机器人

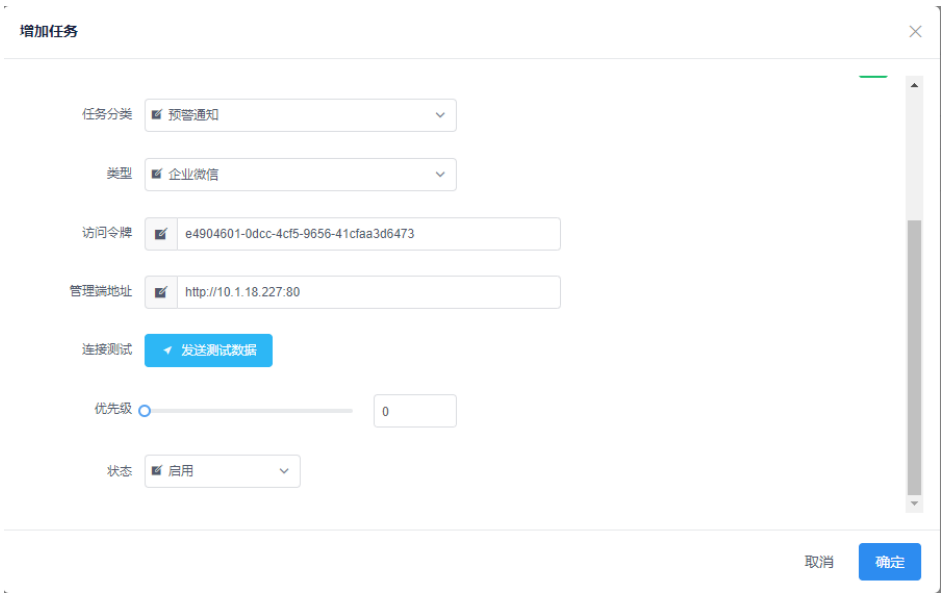
在企业微信群组里添加机器人之后，可以在机器人信息页看到该机器人特有的 webhook 地址。

如上图，假设机器人的 webhook 是：

https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=e4904601-0dcc-4cf5-9656-41cfaa3d6473

那么，在 DecoyMini 预警策略的“访问令牌”就填写以上路径里 key 的值：e4904601-0dcc-4cf5-9656-41cfaa3d6473

管理端地址：配置管理端地址后，在预警信息里支持一键跳转打开对应的风险事件详情。



配置完毕后，点击“发送测试数据”按钮测试参数是否配置正确，若企业微信能够正确收到预警消息，则配置完成。

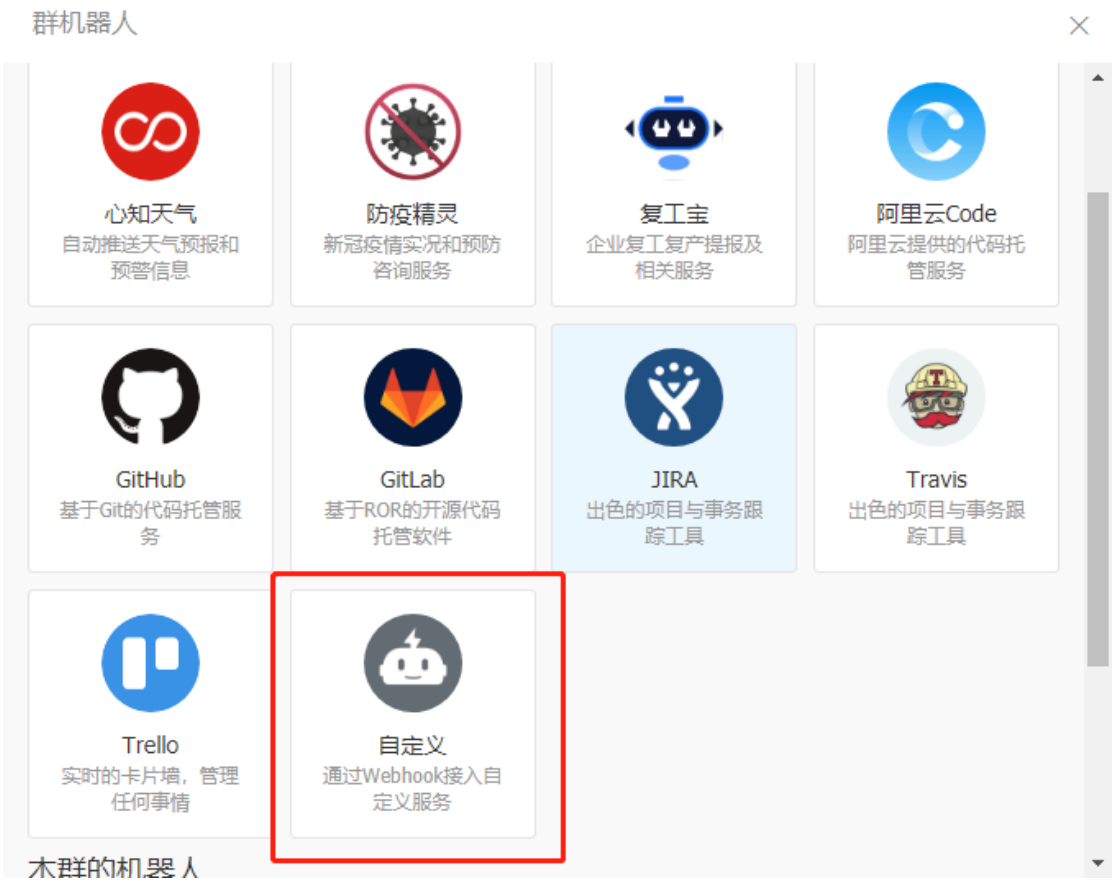
注意：要保护好机器人的 webhook 地址，不要分享到 github、博客等可被公开查阅的地方，避免泄漏！

3.5.2 钉钉接入

1、添加群机器人

选择需要添加机器人的群聊，然后依次单击群设置>智能群助手>添加机器人，选择“自定义”机器人。


预警通知测试群
事件名称: VNC诱捕到Login
目的IP: 10.1.18.234
源IP: 172.16.100.101
类型: svc
级别: 中
描述: 尝试登陆认证
事件ID: BjFtjbc7thz2SQYg
时间: 2021-08-24 14:18:0
查看详情: http://10.1.18.23
圈子
益起动
群接龙
更多
智能群助手
小钉
钉钉官方机器人，提供丰富的技能
已开启的技能
日程提醒
投票提醒
预警通知
通过Webhook接入自定义服务
添加机器人
多款丰富的精选机器人



输入机器人名字并选择要发送消息的群。

完成必要的安全设置，勾选“我已阅读并同意《自定义机器人服务及免责条

款》”，然后单击完成。

点击查看机器人信息可查看到该机器人特有的 Webhook 地址。

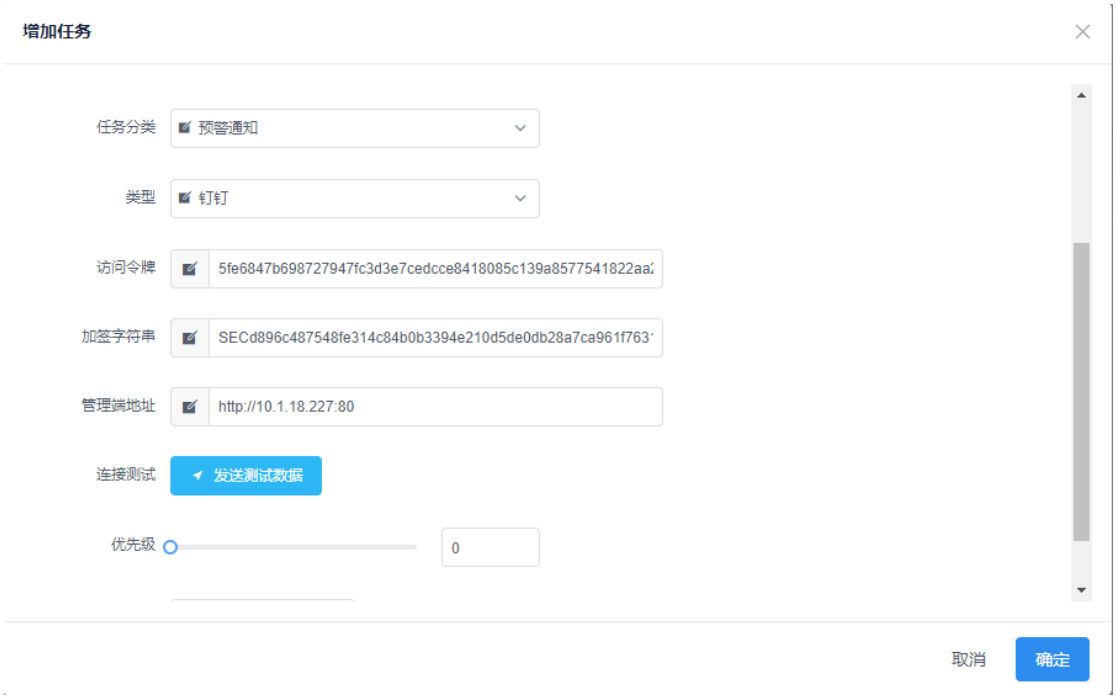
2.使用自定义群机器人

如下图，假设机器人的 webhook 是：

https://oapi.dingtalk.com/robot/send?access_token=5fe6847b698727947fc3d3e7cedcce8418085c139a8577541822aa28e2d9c4a3

那么，系统里预警策略的“访问令牌”就填写以上路径里 access_token 的值：5fe6847b698727947fc3d3e7cedcce8418085c139a8577541822aa28e2d9c4a3

如在设置钉钉群机器人时选择了“加签”，则将加签的密钥填进系统里的“加签字符串”位置，可以配置上管理端地址，配置后在预警信息里支持一键跳转打开对应的风险事件详情。



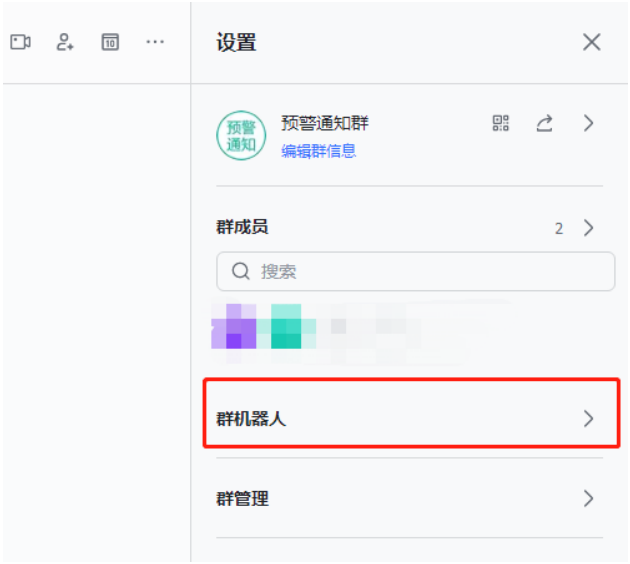
点击“发送测试数据”按钮可进行测试。

注意：请保管好此 Webhook 地址，不要公布在外部网站上，泄露后有安全风险。

3.5.3 飞书接入

1、添加群机器人

选择需要添加机器人的群聊，然后依次单击群“设置”>“群机器人”>“添加机器人”，选择“自定义机器人”。



输入“机器人名称”和“描述”，点击“增加”。

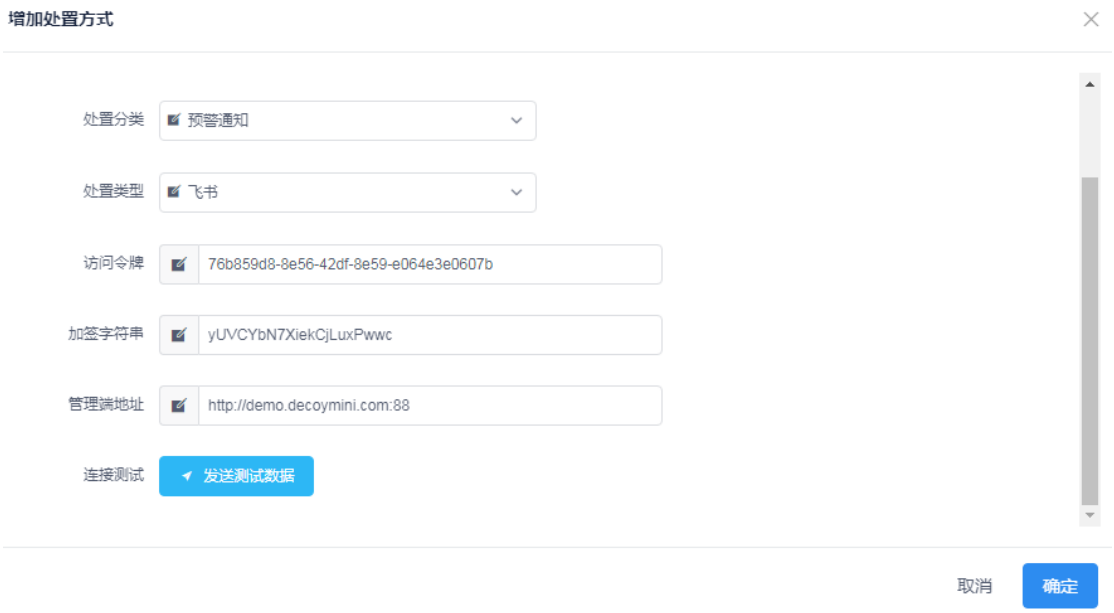
完成必要的“安全设置”：可以按需启用“自定义关键词”，“签名校验”等安全策略，保存好 webhook 地址、签名密钥备用。

完成以上操作后，点击“完成”按钮应用配置。

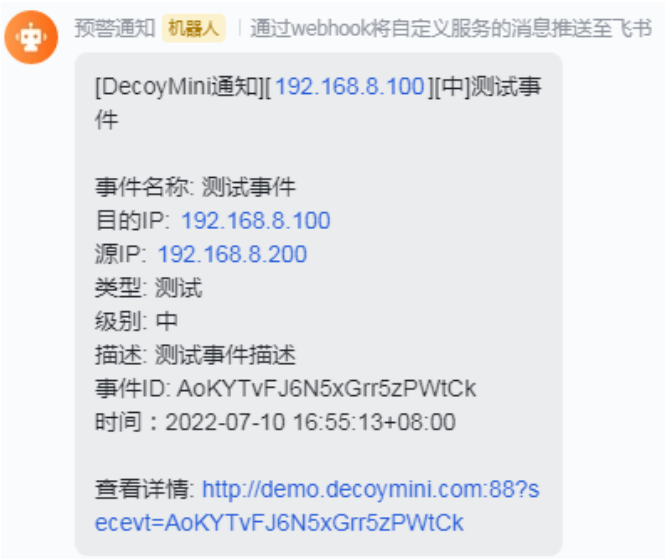
2.使用自定义群机器人

在 DecoyMini 预警策略里，处置类型选择“飞书”，配置对应的参数：

- 访问令牌：假设机器人的 webhook 是：https://open.feishu.cn/open-apis/bot/v2/hook/76b859d8-8e56-42df-8e59-e064e3e0607b，访问令牌填写路径 open-apis/bot/v2/hook/后的值：76b859d8-8e56-42df-8e59-e064e3e0607b；
- 加签字符串：若在设置群机器人时选择了“签名校验”，则将签名校验的密钥填进系统里的“加签字符串”位置；
- 管理端地址：配置管理端地址后，在预警信息里支持一键跳转打开对应的风险事件详情。



点击“发送测试数据”按钮，测试参数是否配置正确，若飞书能够正确收到预警消息，则配置完成。



注意：请保管好此 Webhook 地址，不要公布在外部网站上，泄露后有安全风险。

4 节点

节点提供对诱捕探针节点进行集中管理以及对节点分组进行维护的功能。

4.1 节点管理

本节主要介绍节点管理功能，主要包含节点信息查看、节点信息修改、节点策略运行情况查看等功能。点击 "节点" --> "节点管理" 打开节点管理页面，如下图所示：

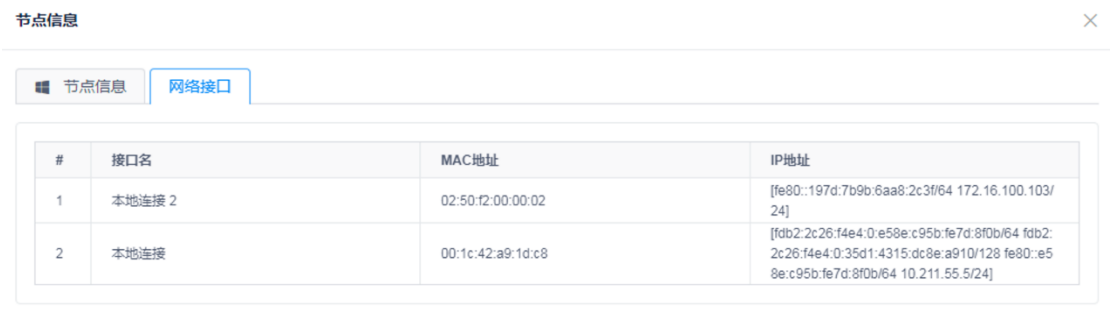
新安装的节点将会自动出现在节点列表里。选择某一个节点，双击或者点击操作列的 "详情" 按钮，可以查看该节点的详细信息，如下图所示：

资产信息包括如下属性：

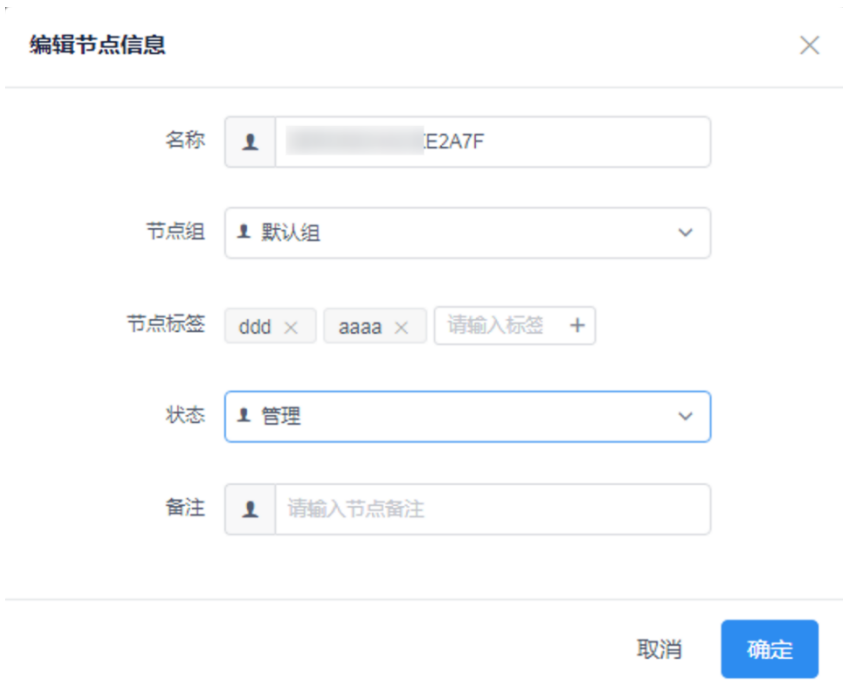
- 名称；
- IP；
- MAC；
- 系统信息；
- 节点组；
- 在线状态；
- 上线时间；
- 注册时间；
- 版本信息；

对不再需要管理的节点，可以点击 "注销" 按钮来注销该节点，注销的节点系统将不再对其进行管理，不再接收该节点上报的数据。

点击 "网络接口" 标签页可以查看该节点所有可用网络接口信息列表，如下所示：



点击节点操作列 "修改" 按钮，可以修改该节点的名称、分组、标签、状态等基本信息：



对于注销的节点，可以点击 "激活" 按钮来激活对应节点，以继续对其进行管理。

对于不再使用的节点，可以点击“删除”按钮来将此节点相关数据从系统里清除。提示：删除的节点以及关联数据删除后将不能恢复，请谨慎操作。

4.2 节点分组

本节主要介绍节点分组配置管理功能，点击 "节点" --> "节点分组" 打开如下页面：

点击左上角的 "新建" 按钮可以新增分组，如下图所示：

新增区域支持的配置的参数包括：

- 组 ID；
- 组名称；
- 上级组；
- 参数；
- 描述；

点击分组操作列 "修改" 按钮可修改分组信息，点击分组操作列 "删除" 按钮可删除对应分组。

5 系统

本节介绍系统的各项配置管理功能。

5.1 参数配置

提供对系统参数进行配置的功能，主要包括以下几部分：安全配置、环境配置、数据存储、预警模板、情报查询等，如下图所示：

以下介绍部分重要的参数：

- **安全配置 /允许登录的论坛用户名**：配置允许登录系统的论坛账户，默认系统仅允许首个登录此系统的论坛账户来登录系统；如果需要多个用户都可以登录此系统，则可以将对应的论坛用户名配置进去，多个用户名之间用;（分号）分割，直接填写*（星号）则允许所有论坛账户登录访问；
- **安全配置 / 有效管理 IP 范围**：设定有效管理 IP 地址，该 IP 可以为单个 IP 地址 (如 192.168.1.126)，也可以包含 * 来对 IP 进行泛匹配 (如 192.168.1.*)，表示将 IP 为 192.168.1.1-192.168.1.254 范围内的所有主机都设置为受信任的管理终端。默认可信管理端配置为空，所有 IP 都可以访问；当配置了 IP 地址后，只有在范围内的 IP 才能连接

管理端；

- **环境配置 / 诱捕探针访问心跳服务地址**：如果诱捕探针不能用默认的访问地址与心跳服务进行通信，则需要手动配置诱捕探针能够访问管理节点心跳服务的有效地址和端口，格式如：10.1.3.8:1226；
- **环境配置 / 本地物理位置**：配置系统里本地 IP 地址显示的 IP 所在地，建议配置为所在地的城市名称即可；
- **环境配置 / 本地物理位置经纬度**：配置本地 IP 地址在风险态势大屏地图上显示的地理位置，具体地址的经纬度可以通过百度等搜索引擎查询后填入，格式为 东经,北纬，例如北京的经纬度值配置为 116.20,39.56；
- **环境配置 / 本地 IP 地址范围**：本地局域网使用的 IP 地址范围，系统默认配置为 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 ，如果本地网络还使用了其他网段的 IP 地址，则只需将 IP 地址段采用“IP/掩码位数”格式用,（逗号）分割追加到当前配置字符串后即可。

5.2 系统信息

点击 "系统" --> "系统信息" --> "系统信息" 标签页，打开系统信息展示页面，在页面上展示有系统基本信息、版本信息等，如下图所示：

5.3 自动升级

配置系统自动升级配置，点击 "系统" --> "系统信息" --> "自动升级" 标签页，打开自动升级配置界面，如下图所示：

配置系统升级相关的参数：

- 升级服务器地址：互联网上升级服务器的地址（默认为：http://s.decoyit.com/upgrade/update），如果地址不可达，则自动升级会失败；
- 升级时间： 24 小时制，如设置为 00:30，表示在下一个凌晨 0 点 30 分的时候开始检查升级、如发现有新的升级包将自动下载进行升级；

可以点击“ 

”，系统会连接升级服务器来检查是否有更新的版本，如果有更新的版本将自动下载进行升级。

升级完成后，管理节点可以在“系统信息”标签页查看升级后的版本信息，诱捕探针节点升级后的版本信息可以在节点管理里对应的节点详细信息里查看。

5.4 手动升级

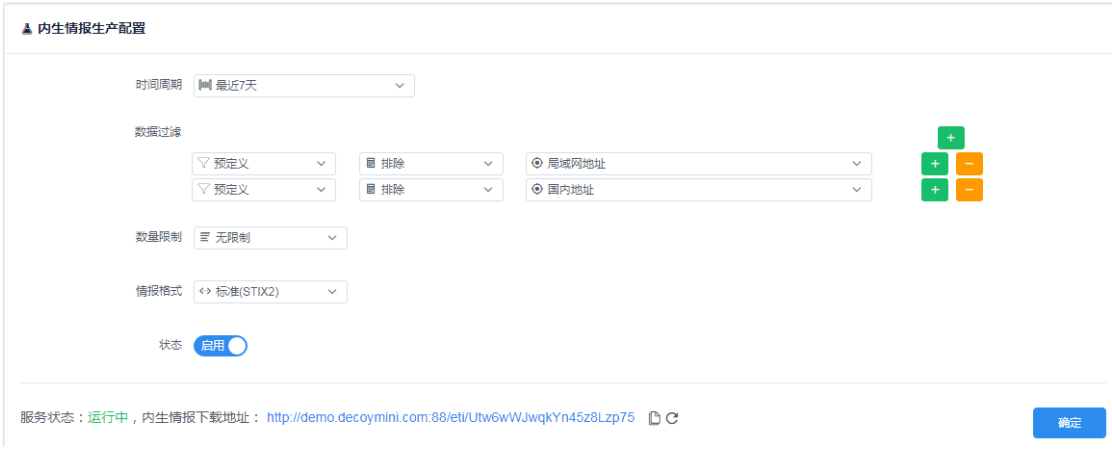
点击 "系统" --> "系统信息" --> "手动升级" 标签页，打开手动升级配置界面：

点击 "请选择升级包文件"，选择升级包在本地存储的路径，点击 "确定" 按钮， 系统会自动上传升级包，然后开始升级。

升级完成后，管理节点可以在“系统信息”标签页查看升级后的版本信息，诱捕探针节点可以在“节点管理”里对应的节点详细信息里查看升级后的版本信息。

6 内生情报

内生情报是威胁情报体系重要组成部分，是外部情报重要的情报能力补充。DecoyMini 基于对攻击源的分析和过滤，支持输出内生情报，可以应用到网关等设备上对攻击进行及时封堵，应用到分析平台上协助对攻击进行发现和分析，利用内生情报可以有效提高对本地攻击的监测、预警和响应能力。



点击“内生情报”菜单，配置内生情报输出规则，配置的主要参数说明如下：

- 时间周期：分析的有效数据周期；
- 数据过滤：配置 IP 过滤规则，支持三种过滤方式：
  - 预定义：可以配置包含或排除局域网地址、国内地址
  - IP 地址段：可以配置包含或排除指定 IP 地址段 IP，多个 IP 段之间用,分割，例如：192.168.1.100,10.0.0.0/8,172.16.0.0/12
  - IP 归属地：可以配置包含或排除指定 IP 归属地（国家名称）的 IP，多个 IP 归属地之间用,分割，例如：美国,英国
- 数量限制：输出的情报数量限制
- 情报格式：输出的情报格式，支持精简、标准 STIX2 格式输出
- 状态：是否启用内生情报服务

当配置完内生情报生产配置，开启情报服务后，就可以通过浏览器访问情报下载地址，或者通 HTTP GET 情报下载地址来下载内生情报数据。

7 技术论坛

DecoyMini 技术论坛（https://bbs.decoymini.com）是一个大家分享 DecoyMini 使用心得、交流欺骗防御技术的平台。当 DecoyMini 系统以论坛账户登录后，通过“技术论坛”菜单可以一键快速跳转到 DecoyMini 技术论坛。欢迎大家在使用 DecoyMini 过程中，登录论坛反馈意见建议、参与交流讨论。

部分板块访问链接如下：

- 提交 BUG：https://bbs.decoymini.com/forum-41-1.html
- 提交 Decoy 情报：https://bbs.decoymini.com/reportTi.php
- 分享仿真模板：https://bbs.decoymini.com/template.php
- 技术分享交流：https://bbs.decoymini.com/forum-53-1.html